Internet Governance Forum (IGF) 2015: Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence Against Women

EDITORS' NOTE (8 December 2015)

This is the fourth and final document ('Draft F') produced by a community of participants in this Internet Governance Forum (IGF) best practice forum (BPF) on online abuse and gender-based violence against women in 2015. This is considered a living document and can still be updated and changed as additional input and comments are received.

How was this document produced?

The IGF provided a unique platform for the collaborative work of this BPF, which aimed to collect the views of the broader Internet governance community on the topic of how to protect the rights of women and girl's rights online and offline by countering online abuse and gender-based violence. The IGF strives in all of its work to provide a neutral and open platform that ensures that all interested parties in the multistakeholder Internet governance community can contribute in a bottom-up fashion.

Draft F was produced as a reflection of this open, iterative and bottom-up process in which people from diverse regions and stakeholder groups participated by completing a survey, attending frequent virtual meetings, commenting on Draft I (which was published on an open and editable Google doc), commenting on Draft II (which was published on the IGF's review platform), commenting on Draft JP (at IGF 2015 and via email), responding to mailing list questions, participating in a social media campaign, and submitting both formal and informal case studies.

For additional background and information on how to participate in this process, please visit the IGF website.

EXECUTIVE SUMMARY

The Internet Governance Forum (IGF) best practice forum (BPF) on Online Abuse and Gender-Based Violence Against Women used an open and inclusive process to gather a variety of views and inputs on the multidimensional issue of online abuse of women and gender-based violence. As a result of this community-driven approach and the mixed methodology the BPF adopted, the BPF's findings reflect a rich diversity of responses from various stakeholders and regions regarding the issue.

The work of this BPF is aimed at being one step in the direction of getting stakeholders to take proper cognisance the issue. The process has also demonstrated the need for more work to be done to understand and address online abuse and gender-based violence and to develop effective responses. The BPF's major findings, along with related recommendations for further research, are summarised below.

Towards a more comprehensive understanding

The BPF's work showed that online abuse and gender-based violence against women are not only interpreted and approached differently in diverse regions, but also that the terminology used for it is inconsistent. The BPF's findings therefore highlight the need for more work to be done towards finding a comprehensive yet flexible definition of the issue that can receive wider recognition around the world.

Various underlying factors play a role in enabling online abuse and gender-based violence. They can also have a compounding effect on the impact of such abuse and violence, as well as the allocation and effectiveness of resources to ensure women gain access to justice and redress. The BPF found that both definitions and initiatives have to address specificities in contexts and relevant circumstances (such as the affected community); all of which are characterised by different obstacles.

Online abuse and gender-based violence have to be studied whilst keeping offline/physical environments, and potential repercussions in offline/physical environments, in mind. The need to understand and address the underlying causes that contribute to and enable such abuse and violence – specifically existing gender inequalities – is also of critical importance in ensuring a more comprehensive understanding of the issue. This reinforces the importance of awareness and literacy programmes, along with substantial investment in research and statistics on the incidence of the issue.

The BPF also found other areas that compel further study and research, including the specific challenges that women with disabilities face, as well as how online abuse and gender-based violence affect girls (below 18 years of age).

Towards a more careful balancing of all the rights and interests involved

Although great strides have been made to improve connectivity and Internet access around the world, growing access has also resulted in the increased use of technology to infringe human rights online; reducing the Internet's potential for development. And while it is now widely recognised that 'offline' human rights apply equally online, the BPF results indicate an apparent discordance when the related obligations on stakeholders to protect and uphold these rights are concerned on the issue of online abuse and gender-based violence.

There is a need for measures to consider, include and balance multiple rights, and to take into account existing inequalities and discrimination that may affect how rights are protected and recognised. In addition, tensions that arise when issues related to multiple rights and interests are involved (including freedom of expression, privacy and anonymity) also need further study.

Considerations in developing responses

Abuse and gender-based violence against women, whether perpetrated online or offline, is difficult to address because of the attitudes, stereotypes and beliefs that underpin the issue. In an online context, such efforts are further complicated because responses need to be implemented within the global context of the Internet and with the cooperation of a multitude of stakeholders.

The BPF found that efforts to develop, encourage and implement practices to counter online abuse and gender-based violence vary significantly around the world. Whilst the BPF did not have the scope to investigate all of the relevant strategies and approaches to the issue, it did manage to highlight many examples of responses taken in the public and private sector, as well as by multistakeholder and community-driven communities. It also extracted various lessons that could be learnt from such approaches and ideas that can be explored in further work.

The BPF found that it is critical that public and private sector approaches to the issue be developed transparently in due consultation with current users (including victims and survivors of online abuse and/or violence) and civil society organizations, and to also consider the needs of future users as Internet access and adoption expand globally.

Where countries consider developing legislative responses to the issue, it is important that relief and redress be prioritised over criminalisation. Not only do governments need to prioritise the access that victims and survivors of online abuse and gender-based violence have to justice, but flexible and informal (yet also transparent) measures that can more easily, quickly and effectively respond to online behaviour need to be investigated in future research.

The BPF encountered much uncertainty regarding intermediaries' responsibilities in addressing and countering the issue. There is therefore a need for the public sector to evaluate its legal relationship with intermediaries in this regard, including the level of obligations it can realistically impose on intermediaries.

While the responsibility of educating users and improving digital literacy levels arguably lies primarily with the public sector, BPF participants also suggested that the public sector should consider cooperating more closely with the private sector (particularly digital intermediaries) to ensure education also continues on relevant platforms.

Lastly, Internet intermediaries can explore clearer and more explicit commitments to comprehensive human rights standards to better address the issue of online abuse and gender-based violence. Existing legal frameworks can provide guidance on the actions they can take to ensure that women's rights online are promoted and respected in compliance with international human rights standards.

First steps

The work of this BPF is both timely and instructive in the context of increasing efforts being invested by different stakeholders at national and global levels to understand and address the issue of online abuse and gender-based violence. It has showed that there are no one-size-fits all solution, and that greater study is needed to further investigate the range of acts, underlying causes, diversity and breadth of impact, and potential responses that can be developed for the issue.

The BPF's work has facilitated diverse stakeholder engagement on the issue, and as such, benefitted from different views and perspectives. This is, however, only a first step towards a more comprehensive understanding and response. It is hoped that some of the findings and areas for further exploration can inform continued discussion and efforts: both at the IGF as a critical platform for multistakeholder engagement on key internet policy, governance and human rights issues, and in other policy discussion spaces.

CONTENTS

INTERPRETATION NOTES

Reading this document

Draft F is divided into three sections – Part I, which contains the results of the best practice forum (BPF)'s work; Part II, which contains relevant background, a detailed description of the BPF's scope, mandate, and methodology followed; and Part 3, which contains five Appendices.

To understand and correctly interpret the contents in Part I, it is necessary to know more about how and why the BPF was created, how the Internet Governance Forum (IGF) operates, and the ways in which the BPF approached its mandate as a multistakeholder community. Readers are therefore strongly advised to also read Part II in order to understand and correctly interpret the results contained in Part I.

Definitions

For the purposes of this document, unless specifically otherwise defined:

- All references to 'women' should be construed as including 'girls' unless otherwise noted. Women of diverse sexualities and gender identities including transgender women are also included in relevant sections of the document.
- 'Girls' is defined as female individuals from birth to the age of 18.
- 'Gender' refers to the social attributes and opportunities associated with being male and female and the relationships between women and men and girls and boys, as well as the relations between women and those between men. These attributes, opportunities and relationships are socially constructed and are learned through socialisation processes. They are context/time-specific and changeable. Gender determines what is expected, allowed and valued in women or men in a given context. Gender is part of broader socio-cultural contexts, intersecting with other factors such as class, race, poverty level, ethnic group and age.
- 'Online abuse and gender-based violence' refers to a range of acts and practices that either occurs online, or through the use of information and communications technologies. It falls within the definition of gender-based violence under General Recommendation 19 of the Committee on the Elimination of Discrimination against Women (CEDAW) convention; that is, 'violence that is directed against a woman because she is a woman or that affects women disproportionately. It includes acts that inflict physical, mental or sexual harm or

suffering, threats of such acts, coercion and other deprivations of liberty.'[1] Recognising the rapidly changing landscape of information and communications technologies (ICTs) that affect the expression of such abuse and violence, this definition is not intended to be exhaustive or definitive, but rather facilitative; to gather best practices and emerging research and analyses in understanding the issue.

- 'Internet governance' is defined using a working definition adopted by the Working Group on Internet Governance (2005),[2] namely: 'the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.'

Abbreviations and acronyms

The following acronyms and abbreviations are used in this document:

APC	Association for Progressive Communications
BPF	best practice forum
CEDAW	Committee on the Elimination of Discrimination against Women
ECOSOC	Economic and Social Council
ICT	Information and communications technology
IGF	Internet Governance Forum
ITU	International Telecommunications Union
LBT	lesbian, bisexual and transgender
LGBT	lesbian, gay, bisexual, transgender and transsexual
MAG	Multistakeholder Advisory Group
STEM	Science Technology Engineering and Mathematics
UGC	user-generated content
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNGA	United Nations General Assembly
UNHRC	United Nations Human Rights Council
VAW	violence against women
WGIG	Working Group on Internet Governance
WSIS	World Summit on the Information Society

[1] Committee on the Elimination of Discrimination Against Women (CEDAW) (1992). *General Recommendation No. 19 (11th session, 1992): Violence against women.* Available online: http://www.un.org/womenwatch/daw/cedaw/recommendations/recomm.htm#recom19. [Accessed 2 November 2015].
[2] WGIG (2005). *Report of the Working Group on Internet Governance*. (Château de Bossey). Available online: http://www.wgig.org/docs/WGIGREPORT.pdf. [Accessed 28 October 2015].

PART I - FINDINGS

A. INTRODUCTION

1. Human rights and freedoms apply both offline and online;[3] not only endowing Internet users with certain freedoms, but also imposing certain obligations for users to respect the rights and freedoms of other Internet users. Although great strides have been made to improve connectivity and Internet access around the world, resulting in expanded opportunities for advancing rights, growing access has also resulted in the increased use of technology to perpetrate acts of abuse and/or violence against users; often resulting in the infringement of human rights online.

2. While violations of users' rights online may affect all users in differing ways, incidents of online abuse and gender-based violence rest on existing disparity and discrimination. Gender-based violence is a "manifestation of historically unequal power relations between women and men, which have led to domination over, and discrimination against, women by men and to the prevention of the full advancement of women".[4]

3. Online abuse and gender-based violence is understood as being a part of gender-based violence. In addition to existing structural inequality and discrimination between genders, disparity in access to, participation in and decision-making over the Internet and technology development are all factors that play a part in its manifestation online and through the use of information and communications technology (ICT).[5] As such, online abuse and gender-based violence disproportionately affect women in their online interactions; encompassing acts of gender-based violence such as domestic violence, sexual harassment, sexual violence, and violence against women in times of conflict, that are committed, abetted or aggravated, in part or fully, by the use of ICTs.

4. Over the past few years, increasing attention has been paid to understanding the nature, harm and consequences of online abuse and gender-based violence by the media (including journalists and citizen journalists), governments and women's

[3] For example: United Nations Human Rights Council (UNHRC) (29 June 2012). *The Promotion, Protection and Enjoyment of Human Rights on the Internet* (A/HRC/20/L.13). Available online: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280. [Accessed 28 October 2015].
[4] Council of Europe (2014). *Convention on Preventing and Combating Violence Against Women and Domestic Violence.* Available online: http://conventions.coe.int/Treaty/EN/Treaties/Html/210.htm. [Accessed 30 October 2015].
[5] For example, a Broadband Commission report estimated that in 2013, there are 200 million fewer women online than men, a gap which can grow to 350 million in the next three years if no action is taken [See: Broadband Commission (2013), *Doubling Digital Opportunities: Enhancing the Inclusion of Women and Girls in the Information Society*. Available online: http://www.broadbandcommission.org/documents/working-groups/bb-doubling-digital-2013.pdf. [Accessed 2 November 2015].

movements. This is evidenced by the formal recognition of online abuse and gender-based violence in significant women's rights policy spaces and the focus on secure online practices for women and women human rights defenders. For instance, the United Nations (UN) Secretary General's *In-depth study on all forms of violence against women*[6] noted in 2006 that:

> *'More inquiry is needed about the use of technology, such as computers and cell phones, in developing and expanding forms of violence. Evolving and emerging forms of violence need to be named so that they can be recognized and better addressed.'*

5. At the end of 2013, the UN General Assembly (UNGA) also adopted a consensus resolution[7] on protecting women human rights defenders with language on technology-related human rights violations:

> *'... information-technology-related violations, abuses and violence against women, including women human rights defenders, such as online harassment, cyberstalking, violation of privacy, censorship and hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights.'*

6. Despite these developments at international organization levels, the importance of addressing online abuse and gender-based violence has arguably not been adequately taken up by several of the stakeholders within the Internet governance ecosystem.[8] There is still a lack of awareness regarding what kinds of online conduct constitute abusive and/or gender-based violent behaviour and the variety of actions that can be taken to address and prevent such abuse and violence.

7. Taking effective action to counter online abuse and gender-based violence is not only important in ensuring that the Internet fulfils its potential as a positive driver for change and development, but also in helping to construct a safe and secure environment for women and girls in every sphere of life. Online abuse and gender-based violence can, among other things, limit women's ability to take advantage of the opportunities that ICTs provide for the full realisation of women's human

---

[6] United Nations General Assembly (UNGA) (6 July 2006). *In-depth study of all forms of violence against women.* (A/61/122/Add.1). Available online: http://www.un.org/womenwatch/daw/vaw/SGstudyvaw.htm. [Accessed 29 October 2015].

[7] UNGA (30 January 2014). *Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: Protecting women rights defenders.* (A/RES/68/181). Available online: http://www.gender.cawater-info.net/publications/pdf/n1345031.pdf. [Accessed 2 November 2015].

[8] As defined by the Working Group on Internet Governance (WGIG) (2005). *Report of the Working Group on Internet Governance*. (Château de Bossey). Available online: http://www.wgig.org/docs/WGIGREPORT.pdf. [Accessed 28 October 2015]. Also see Interpretation Notes above.

rights, act as a barrier to access that can exacerbate the gender digital gap, often violate women's human rights, and reaffirm and reproduce gender stereotypes. Online abuse and gender-based violence are aggravated by various obstacles that prevent women from exercising their right to access justice in both online and offline environments, including a lack of effective and timely remedies to address online abuse and gender-based violence experienced by women, and obstacles faced in collecting evidence relating to such abuse and violence.[9]

8. To help address this challenge, the Internet Governance Forum (IGF) has brought together multiple stakeholders from diverse communities to investigate the types of conduct that potentially constitute online abuse and gender-based violence, the underlying factors that contribute to enabling environments for online abuse and gender-based violence, the impact that online abuse has on individuals and in communities, other related contentious issues, and emerging solutions, responses and/or strategies that constitute good and/or best practices and provide insights and lessons to inform future work aimed at countering online abuse and gender-based violence.

9. This draft report is the result of nine months of deliberations using a methodology defined in Part II below. It was produced as part of an ongoing, open and iterative process in which multiple people from diverse regions and stakeholder groups participated.

10. In discussing the BPF's results, Part I includes a broad and flexible problem definition; the underlying factors and enabling environments that facilitate and enable abuse of women and gender-based violence online (including how new environments and users should be protected in debates around access and connectivity); the careful exercise of balancing fundamental rights and interests in protecting women from online abuse and gender-based violence; the impact and consequences of abuse of women and gender-based violence online; the variety of responses and measures that have been used by stakeholders to address the issue; and conclusions (including recommendations for future work and research).

[9] See: CEDAW (23 July 2015). *General recommendation on women's access to justice* (C/CG/33). Available online: http://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_33_7767_E.pdf [Accessed 28 October 2015].

B. PROBLEM DEFINITION

11. Online abuse and gender-based violence refer to a range of acts and practices that either occurs online, or through the use of ICTs, which fall within the definition of gender-based violence under General Recommendation 19 of the CEDAW convention:[10]

> *"violence that is directed against a woman because she is a woman or that affects women disproportionately. It includes acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion and other deprivations of liberty".*

12. Recognising the rapidly changing landscape of ICTs that affect the expression of such abuse and violence, this definition is not intended to be exhaustive or definitive, but facilitative; to gather best practices and emerging research and analyses in understanding the issue. The BPF instead studied existing definitions along with the examples of behaviour that might, under specific circumstances, constitute abuse, and the contexts in which such violations are more likely to occur. This is also intended to support and inform existing efforts towards building knowledge and awareness regarding the types of actions that constitute online abuse and gender-based violence with the aim of developing responses.

13. See Section G (Conclusion) for the BPF's recommendations in terms of defining the problem in the future.

i. Existing definitions

14. While there are no formally recognised definitions, some efforts have been made to define the issue of online abuse and gender-based violence, albeit using terms that are not synonymous but similar (e.g. terms like cyber violence, online violence and technology-related violence against women). These policy documents and research initiatives provide some guidance in delineating the dimensions of this issue.

15. The UN HRC consensus resolution *The promotion, protection and enjoyment of human rights on the Internet* affirmed that the same rights that people have offline must also be protected online.[11] There are also numerous international human rights instruments and documents that state clearly that all forms of gender-based

[10] CEDAW (1992). *General Recommendation No. 19 (11th session, 1992): Violence against women.* Available online: http://www.un.org/womenwatch/daw/cedaw/recommendations/recomm.htm#recom19. [Accessed 2 November 2015].
[11] UN HRC (29 June 2012). *The Promotion, Protection and Enjoyment of Human Rights on the Internet* (A/HRC/20/L.13). Available online: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280. [Accessed 28 October 2015].

violence amount to discrimination, and seriously inhibit women's ability to enjoy their human rights and fundamental freedoms. This includes acts of gender-based violence that are experienced online or expressed through the use of ICTs. A few examples include:

16. Article 1 the Declaration on the Elimination of Violence against Women[12] defines **violence against women** to mean:

> *'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.'*

17. Article 3 of the Council of Europe Convention on preventing and combating violence against women and domestic violence defines **violence against women** as:

> *'a violation of human rights and a form of discrimination against women and shall mean all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.'*

18. A report by Women's Aid[13] looked into online harassment, stalking and abuse and defined **online abuse** as:

> *'the use of the internet or other electronic means to direct abusive, unwanted and offensive behaviour at an individual or group of individuals.'*

19. Research by the Association for Progressive Communications (APC)[14] defines **technology-related violence** as encompassing:

> *'acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as phones, the internet, social media platforms, and email.'*

---

[12] UNGA (20 December 1993). *Declaration on the Elimination of Violence against Women* (A/RES/48/104). Available online: http://www.un.org/documents/ga/res/48/a48r104.htm. [Accessed 29 October 2015].
[13] Women's Aid (September 2013). *Virtual World: Real Fear: Women's Aid Report into Online Abuse, Harassment, and Stalking*. Available online: http://www.womensaid.org.uk/page.asp?section=00010001001400130007&sectionTitle=Virtual+World+Real+Fear. [Accessed 29 October 2015].
[14] Association for Progressive Communications (APC) (2 March 2015). *From Impunity to Justice: Exploring Corporate and Legal Remedies for Technology-Related Violence Against Women.* Available online: http://www.genderit.org/articles/impunity-justice-exploring-corporate-and-legal-remedies-technology-related-violence-against. [Accessed 29 October 2015].

20. The recently published (and subsequently withdrawn, pending updates) UN Broadband Commission for Digital Development Working Group on Broadband and Gender report[15] defines **cyber violence** against women to include:

> *'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.'*

ii. Perpetrators and victims

21. Women do not have to be Internet users to suffer online violence and/or abuse (e.g. the distribution of rape videos online where victims are unaware of the distribution of such videos online). On the other hand, for many women who are active online, online spaces are intricately linked to offline spaces; making it difficult to differentiate between experiences of events that take place online versus events offline events.[16]

> *"Everyone who uses the Internet is potentially affected, it is a serious and a growing problem by all accounts."*
>
> **BPF survey respondent from the UK**

22. The identification of 'victims' and 'survivors' is difficult (if not unfeasible) in a context where there is still a serious lack of awareness about the impact of online violations on women's rights (as is also indicated by the survey results[17]). This lack of awareness not only reinforces the importance of sensitisation, awareness raising, and literacy programmes on the topic, but it also makes it difficult for

[15] Broadband Commission (September 2015). *Cyber Violence against Women and Girls: A world-wide wake-up call.* Note that at time of publication of Draft F, the report had been withdrawn with the aim to update and fix mistakes. As at 26 November 2015, the report remained available online at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259. [Accessed 29 October 2015].
[16] E.g. page 6, End Violence Against Women Coalition (EVAW) (2013). *New Technology, Same Old Problems.* Available online: http://www.endviolenceagainstwomen.org.uk/data/files/Report_New_Technology_Same_Old_Problems.pdf. [Accessed 29 October 2015].
[17] Few respondents explicitly recognised that online abuse impacts women's rights. While the survey results are by no means representative of a larger population, the lack of importance that the respondents attached to online abuse and violence as a limitation of women's rights was noteworthy.

victims and survivors to make claims for the fulfilment and enforcement of such rights.[18]

23. The perpetrators of online abuse and gender-based violence, and violations of human rights online, can be male or female. Likewise, men and boys can also be victims of online abuse and violence.[19] However, it is important to note that online abuse and gender-based violence stem from the same existing structural inequalities and discrimination as other forms of gender-based violence; compounded with gender disparity in access to ICTs. This has a significant impact on not only the majority of victims and survivors who face such abuse and violence, but also on the perpetrators involved.

24. A vast proportion of online abuse and gender-based violence tend to happen using anonymous accounts or accounts with pseudonyms and/or false names, making it difficult to identify perpetrators. On the other hand, anonymity is recognised as a valuable tool for women to be able to exercise their rights online, as is discussed in more detail in Section D below.

iii. The impact of context and identity

25. Researchers[20] have identified at least three dimensions of violence against women which are arguably also of relevance in online contexts. These dimensions include a conceptual dimension (physical versus emotional and economic violence), a temporal dimension (episodic versus chronic violence) and an evaluative dimension (differentiate between violence measured by objective standards and violence subjectively perceived by women and men). This research can provide a useful approach to understanding the different dimensions of online and offline violations of women's rights.

26. Potentially abusive online behaviour or violations cannot be viewed in isolation: often one comment, tweet or post, for example, might not be abusive when viewed individually but does become abusive when viewed in context of the frequency,

[18] See: CEDAW (23 July 2014). *General recommendation on women's access to justice* (C/CG/33). Available online: http://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_33_7767_E.pdf [Accessed 28 October 2015].

[19] Pew research indicates that in an American context, men are more likely than women to experience name-calling and embarrassment online, whilst young women are 'particularly vulnerable to sexual harassment and stalking' (or what the report calls 'severe' forms of abuse). The research was done on a randomly selected panel of U.S. adults who self-identify as Internet users in the USA. See Pew Research (2014), *Online Harassment.* Available online: http://www.pewinternet.org/files/2014/10/PI_OnlineHarassment_72815.pdf. [Accessed November 2015].

[20] Example submitted by Agustina Callegari, Personal Data Protection Center for Buenos Aires Ombudsman's Office, Argentina, as part of comments on Draft II (submitted October 2015), see Appendix 4. The research concerned is available in Spanish: Roberto Castro and Florinda Riquer, Cad. Saude Pubilca, Rio de Janeiro, 19(1): 135-146 (2003). *Research on violence against women in Latin America: form blind empiricism to theory without data.* Available online: http://www.scielo.br/pdf/csp/v19n1/14913.pdf/ [Accessed 30 October 2015].

time and prevalence of such behaviour, including whether and how it was accompanied by other media like videos or emails. In the case of online mobbing, for instance, each online comment or post viewed individually might appear harmless, but combined such posts can have a cumulative and deafening result that chill women's freedom of speech, assembly and access to information. Online harassment that systematically targets women – also termed "gendertrolling" – is located within, and is a manifestation of patriarchal culture that requires an assessment of harm and response from this vantage point.[21] Temporality and context therefore pose a significant problem for addressing violations of human rights online, as ordinary measures for addressing abuse do not always take cognisance of such factors and the contexts involved.

27. Online abuse and gender-based violence also affect and impact women in different ways depending on the context or identity. This can be attributed to multiple and intersecting forms discrimination that women and girls face based on these factors. For example, women can be more at risk to diverse types of abusive or violent behaviour because of their profession, age, identity or geographical location. Some of these specific contexts or 'classifications' of women are outlined in the paragraphs below.[22]

28. *Girls and young women*

There is growing recognition of the particular risks that young people and children face online in many countries around the world, including an IGF BPF on the topic in 2014.[23] There are also many programmes that aim to prevent bullying, cyberbullying and promote digital citizenship, like the Amigos Conectados programme in Latin America,[24] Internet Matters in the UK,[25] and Netsmartz Workshop in the USA.[26] But although girls and young women are often more likely to experience certain forms of online abuse and gender-related violence, particularly with respect of their bodily development and sexuality, most of these and other literacy programmes and research into child online protection is not gender-specific.

---

[21] See Katie Klabusich, RH Reality Check (21 October 2015). *'Gendertrolling' and Violence Against Abortion Providers: Cut From the Same Cloth*. Available online: http://rhrealitycheck.org/article/2015/10/21/gendertrolling-violence-abortion-providers-cut-cloth/ [Accessed 31 October 2015].

[22] This list was identified by BPF participants as people who might be particularly vulnerable to online abuse and gender-based violence and is not an exhaustive list.

[23] Internet Governance Forum (IGF) (2014). *Best Practice Forum on Online Child Protection*. Available online: http://www.intgovforum.org/cms/documents/best-practice-forums/best-practices-for-online-child-protection/413-bpf-2014-outcome-document-online-child-protection/file. [Accessed 29 October 2015].

[24] Disney Latino (website). Available online: http://amigosconectados.disneylatino.com/esp/. [Accessed 29 October 2015].

[25] Internet Matters (website). Available online: http://www.internetmatters.org/. [Accessed 29 October 2015].

[26] National Center for Missing and Exploited Children (website). Available online: http://www.netsmartz.org/Parents. [Accessed 29 October 2015].

Example from São Paulo, Brazil[27]
As part of a practice called 'Top 10' in at least two peripheral neighbourhoods of São Paulo, profile pictures of girls aged between 12 and 15 are mixed with phrases describing the girls' alleged sexual behaviour, and the girls are then ranked according to 'how whore they are'. The practice has reportedly led to school dropouts and suicides. The InternetLab, an independent research centre that has done extensive research on the practice, believes the practice to be quite widespread in Brazil.

Example from Pakistan:[28]
A 16 year-old girl in Pakistan was filmed having sex with an older man and repeatedly blackmailed for sex thereafter. Her family were also subsequently blackmailed for money. The girl's father said the incidents had happened because the girl had been granted the 'freedom' to attend school; bringing 'shame and dishonour' to the family.

Example from the Philippines:[29]
Videos of what purports to be a well-known 12 year-old female actor allegedly masturbating in her room were shared online in June 2015. While the identity of the person(s) who uploaded the videos remains unknown, the videos were shared repeatedly on social media platforms. No action appears to have been taken against the perpetrator(s).

29. *Women in rural contexts*

Women in rural contexts face multiple challenges in terms of access to the Internet. This includes access to available and affordable infrastructure, and importantly, different gendered norms that apply when it comes to who is prioritised for accessing and using technology, as well as existing gender disparities such as income and literacy.

As a result, digital divides tend to affect women more than men, and in rural areas even more so and in different ways (also see Section C ii below). Further, women in rural contexts may also be subjected to greater social and cultural surveillance that can result in far greater impact and harm in incidences of online abuse and violence. When compounded with the existing gap in access to and control over technology, this also significantly impacts their capacity to take action and access redress.

[27] Summarised from example and case study submitted on BPF mailing list, Mariana Valenti, InternetLab, Brazil.
[28] Summarised from case study, APC (2014). *Case study: When a sex video is used for blackmail.* Also available online: http://www.genderit.org/sites/default/upload/case_studies_pak3_0.pdf. [Accessed 29 October 2015].
[29] Summarised from case study, Lisa Garcia, Foundation for Media Alternatives, Philippines. See Appendix 3, page 105.

Example from Pakistan:[30]
In a remote Pakistani village, women who had been filmed with a mobile phone whilst dancing and singing together with men at a wedding ceremony were reportedly sentenced to death by a tribal assembly. In this area, strict gender segregation beliefs do not permit women and men to be seen socialising together. The video was disseminated without their knowledge or consent, and had a far-reaching consequence by transmitting a private moment into a more public space.

Example from Mexico:[31]
In a small village in Mexico, an active parishioner and teacher was accused of cheating on her husband, and their children of being fathered by others, on a Facebook page dedicated to gossip in the community. The accusations damaged her reputation in the community, made some parents unwilling to trust her as a teacher, and also led to her being abused by her husband.

30. *Religion, culture and morality*

Women often disproportionately bear the burdens of upholding religious, cultural and moral values of a particular society. As such, they can face additional risk of attacks for being perceived to violate a particular religious, cultural or moral norm. This is especially in relation to issues related to bodily autonomy and sexuality. For example, organizations working on the right to abortion face frequent attacks, which extends to the digital sphere, as noted by the UNGA Resolution on Protecting Women Human Rights Defenders.[32]

Religious, cultural or moral norms can also be used as methods to attack and threaten women online. In some contexts, this can put women especially at risk to physical violence, where the line between online threats and the likelihood of offline occurrence is fine. Access to justice can also be challenging when the state or law enforcement prioritises prosecution of offences against religion, culture and morality rather than online abuse and violence.

Example from India:[33]

[30] Summarised from case study submitted on BPF mailing list, Arzak Khan, Internet Policy Observatory, Pakistan. His summary of story available online at: iPop (6 June 2012). *Death for dancing and mobile phones in Pakistan.* Available online: http://ipop.org.pk/death-for-dancing-and-mobile-phones-in-pakistan/. [Accessed 29 October 2015].
[31] Summarised from case study, APC. *Case study from Mexico: A Defamatory Facebook Profile Brings Violence into Marriages* Available online: http://www.genderit.org/sites/default/upload/case_studies_mex4_0.pdf. [Accessed 29 October 2015].
[32] UNGA (30 January 2014). *Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders* (A/RES/68/181). Available online: http://www.gender.cawater-info.net/publications/pdf/n1345031.pdf. [Accessed 30 October 2015].
[33]Summarised from a paper by the Internet Democracy Project (2013), *Don't let it Stand! An Exploratory Study of Women and Verbal Online Abuse in India.* Available online: http://internetdemocracy.in/wp-

Sonali Ranade is a trader who tweets about a range of issues, from market trends to gender. She faced vicious attacks on Twitter after one of her posts called for the Chief Minister of Gujarat (a state in western India), to make amends for the way in which he handled riots. An analysis of the online attacks reportedly traced it back to an organised effort by the religious Hindu right wing.

Example from Latin America:[34]
The Latin America and Caribbean Women's Health Network faced systematic cracking of their website immediately following the launch of several campaign activities in September 2013 to decriminalise abortion in the region. This was seen as a serious extension of the harassment and intimidation of women's human rights defenders who worked on the issue of promoting women's sexual and reproductive health and rights.

Example from the USA:[35]
The USA's largest reproductive health care provider, Planned Parenthood, faced systematic digital attacks and cracking in July 2015 by self-professed anti-abortion hackers. Attacks included a breach into their encrypted employee database with the stated intention of releasing personally identifiable information of abortion service providers, and disabling of their websites from distributed denial of service (DDoS) attacks. Set within a context where abortion is already stigmatised and morally politicised, the physical threat to safety was underlined through the risk of publicising personal information.

Example from Malaysia:[36]
A radio journalist received numerous threats of violence, rape and murder on social media after presenting a satirical video that questioned the opposition state government's intention to push for Islamic criminal law, or hudud, in Malaysia. The video was removed, and the journalist was probed for so-called 'blasphemy'.

---

content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf. [Accessed 29 October 2015].

[34] See article on incident: Protection Online (21 October 2013). *WHRD IC condemns the aggressive and systematic digital harassment of the Latin America and Caribbean Women's Health Network (LACWHN)*. Available online: http://protectionline.org/2013/10/21/whrd-ic-condemns-the-aggressive-and-systematic-digital-harassment-of-the-latin-america-and-caribbean-womens-health-network-lacwhn-2/. [Accessed 29 October 2015].

[35] See article on incident: Katie Klabusich, Rolling Stone (31 July 2015). *Planned Parenthood Under Attack by Anti-Abortion Hackers, Politicians.* Available online: http://www.rollingstone.com/politics/news/planned-parenthood-under-attack-by-anti-abortion-hackers-politicians-20150731[Accessed 30 October 2015].

[36] See articles on incident: The Malay Insider (22 March 2015). *How is it blasphemous to comment on hudud, asks father of BFM host.* Available online: http://www.themalaysianinsider.com/malaysia/article/baffled-by-investigation-father-of-bfm-host-denies-blasphemy-claim. [Accessed 29 October 2015]. Also see: Victoria Richards, The Independent (1 April 2015). *Rape threats, death threats and police investigation after video poking fun at an Islamic Party in Malaysia goes viral.* Available online: http://www.independent.co.uk/news/world/asia/rape-threats-death-threats-and-a-police-investigation-after-video-poking-fun-at-an-islamic-party-in-10149554.html. [Accessed 29 October 2015].

31. *Women of diverse sexualities and gender identities*

For lesbian, bisexual and transgender (LBT) women who face existing discrimination, stigma and in some contexts, criminalisation and serious threats to their personal safety, the Internet can be an important space for them to exercise their rights. They are able to gain access to critical information that is otherwise restricted or censored, to form communities in relative safety, and to organise for the advancement of their interests and human rights.

Despite this positive potential, studies show that LBT individuals and advocates tend to face more threats and intimidation online.[37] Stonewall, a UK-based organization, has reported that whilst the Internet is a vital source for lesbian, gay, bisexual, transgender and transsexual (LGBT) young people to find information they cannot find at school, one in four of LGBT young people reported experiences of cyberbullying.[38] A global monitoring survey conducted by APC in 2013 found that 51% of sexual rights advocates had received violent messages, threats or comments while working online, while 34% mentioned that they faced intimidation online. In the same study, 45% of respondents indicated serious concerns that their private information online can be accessed without their knowledge or consent.[39]

For LBT women, issues of anonymity and real name policies are also of particular relevance – as is also discussed in paragraphs 78 to 81 below (Section D).

Example from Cameroon:[40]
Activists working on LGBT issues often face threats of violence in Cameroon. A primary method is through intimidation via text messages or Facebook messages, which are often sent anonymously. Threats also extend beyond the advocates, including lawyers and family members. While advocates of all gender and sexual identities are at risk, women face the additional threat of sexualised attacks, including sexual assault. The online threats often escalate to physical violence.

Example from Mexico:[41]

[37] A Dutch study, for instance, showed that lesbians were 6.4% more likely to experience online bullying than heterosexual women. See European Union Agency for Fundamental Rights (FRA) (September 2014). *Violence against women: European Union survey results in the Dutch context*. Available online: http://www.atria.nl/atria/eng/news/publications/_pid/column2_1/_rp_column2_1_elementId/1_347424. [Accessed 30 October 2015].
[38] Stonewall (2014). *Staying Safe Online.* Available online: https://www.stonewall.org.uk/sites/default/files/onlinestaysafe.pdf. [Accessed 30 October 2015].
[39] APC (15 July 2013). *Survey on Sexual Activism, Morality and the Internet.* Available online: http://www.genderit.org/articles/survey-sexual-activism-morality-and-internet. [Accessed 30 October 2015].
[40] France 24 (25 February 2015). *LGBT activists in Cameroon face threats and violence*. Available online: http://www.france24.com/en/20150224-cameroon-lgbt-activists-face-threats-violence. [Accessed 30 October 2015].

When a single lesbian mother disputed a school's decision to keep her son from attending school because of his long hair, she started receiving online threats and abuse that forced her from her home. People started going through her photographs on social media and using them for tweets and other posts to illustrate that she was allegedly an unfit mother who was forcing her son into cross-dressing and 'becoming a homosexual'; and threatened her with death and corrective rape in order to 'protect her son from her'.

32. *Women with disabilities*

While the online abuse and/or violence women with disabilities might face was noted as being of particular importance by some BPF participants, the BPF has yet to receive information that can help to illustrate the specific risks that women with disabilities face online. The area is sufficiently critical to be included as a clear gap where more research and analysis is needed, as is also noted in Section G (Conclusion).

33. *"Public" women and women in technology fields*

Women who are prominent in online or offline environments tend to be subjected to more abuse when they interact or express opinions online. Such cases of abuse often also attract more media attention than the cases of less prominent women. Examples of such prominent women include human rights defenders, women journalists (including citizen journalists and bloggers), and women who are active in technology industries. Women also often face threats and violence after political articulation or participation.

> *"…as soon as I was elected, and I made my first speech in the culture committee, actually defending the Erasmus programme (which should not be particularly contentious), I was subjected to Twitter hate by an extreme right party... Because I was a woman and I dared to speak up, the abuse that I got was actually sexual abuse."*
>
> **Comment by Julie Ward (European Parliament), during BPF session at IGF 2015**

[41] Read more here: Catalina Ruiz-Navarro, Digital Rights: Latin America & Caribbean (27 October 2015). *Trolls and access to rights: the #AxanDecide case.* Available online: http://www.digitalrightslac.net/en/troles-y-acceso-a-los-derechos-el-caso-axandecide/ [Accessed 29 October 2015].

Example from Pakistan:[42]
Bayhaya developed a campaign as part of her work as human rights activist in Pakistan. Following the launch of the campaign she, along with her female colleagues, received serious online threats and abuse. Although she closed her social media accounts, her personal data (including pictures) were stolen and used for posters that accused her of 'blasphemy' and insulting the Quran and Prophet Muhammed.

Example from Britain:[43]
Caroline Criado-Perez took part in a successful campaign to retain a female face on one of the Bank of England's pound notes. As a result she suffered severe online violence, including rape threats and other abuse. Her supporters – including a prominent politician and female journalists – faced similar abuse online.

Example from India:[44]
Sagarika Ghose and her husband, Rajdeep Sardesai, are both well-known journalists and active Twitter users in India. While both receive frequent criticism and abuse on Twitter for their views, the format such abuse takes is notably gendered. The vitriol faced by Sagarika is often sexually violent in nature; one example being: "Bitch, you deserve to be stripped and raped publicly."

Example from the USA:[45]
In August 2014, a series of coordinated and escalating incidents of harassment, which included doxing, threats of violence and rape and death threats, were primarily targeted at prominent and vocal feminists in the field of gaming, including Zoë Quinn, Brianna Wu, and Anita Sarkeesian. The harassment campaign later became synonymous with the name Gamergate; among other things raising awareness of sexism in the gaming industry.

iv. Types of behaviour and/or conduct

34. One of the first tasks involved in defining the BPF's scope of work included outlining the types of behaviour that might constitute online abuse and gender-

[42] Summarised from case study, APC (2014). *Case study from Pakistan: When women's human rights are deemed 'blasphemous'.* Available online: http://www.genderit.org/sites/default/upload/case_studies_pak1_1.pdf. [Accessed 30 October 2015].
[43] Summarised from case study and report submitted by Vera Gray, Operations COORD, UK. See Appendix 3, page 120. The report: EVAW (2013). *New Technology, Same Old Problems.* Available online: http://www.endviolenceagainstwomen.org.uk/data/files/Report_New_Technology_Same_Old_Problems.pdf. [Accessed 29 October 2015].
[44] Summarised from a paper by the Internet Democracy Project (2013). *Don't let it Stand! An Exploratory Study of Women and Verbal Online Abuse in India.* Available online: http://internetdemocracy.in/wp-content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf. [Accessed 30 October 2015].
[45] See, for example, Wikipedia (n.d.).*Gamergate Controversy.* Available online: https://en.wikipedia.org/wiki/Gamergate_controversy [Accessed 26 November 2015].

based violence against women with the effect of violating human rights. This was seen as a critical task by participants because of the perceived lack of awareness regarding this issue. As discussed in Part II (section vi) below, a survey was designed and broadly distributed to ask a range of stakeholders to explain their perception of the problem and to list examples of the types of behaviour that they consider to be within this ambit in their knowledge and/or experience. There were 43 responses from different regions and stakeholder groups who responded to this particular section (see Appendix 2 for the survey questions and analysis).

35. In the survey responses, definitions of online violence against women and girls generally contained three common elements, namely: i) the range of action/ behaviour that constitutes online abuse and gender-based violence; ii) impact on rights and harm experienced; and iii) the role of technology in enacting/enabling online abuse and/or gender-based violence.

36. Many of the examples of online abuse and gender-based violence (discussed in more detail below) cited by survey respondents were similar or overlapping (especially when synonyms are considered). The examples most frequently identified related to infringements of privacy, harassment, surveillance and monitoring, and damaging reputation and/or credibility. Direct threats of violence, blackmail and attacks against communities were less frequently listed as examples of abuse. Some respondents also felt that excluding women from accessing the Internet and/or certain online services because they were female amounted to violations of their human rights.

37. The following non-exhaustive list of online conduct and/or behaviour that potentially constitute abusive behaviour, depending on the aforementioned contexts and other factors in which such behaviour occurs (also see Section C below), has been identified as practices that may constitute forms of online abuse and/or gender-based violence. Note that while conduct has been divided into categories for ease of reference, these categories are not mutually exclusive. It is also important to note that these acts are often an extension of existing gender-based violence, such as domestic violence, stalking and sexual harassment, or targets the victim on the basis of her gender or sexuality.

38. *Infringement of privacy*

- accessing, using, manipulating and/or disseminating private data without consent (by cracking[46] personal accounts, stealing passwords, using/ stealing identities, using another person's computer to access a user's accounts while it is logged in, etc.)

[46] The term 'cracking' is used rather than 'hacking' to indicate a forced entry or takeover of content with malicious intent, while 'hacking' could include similar actions that are *bona fide* and/or done in the public interest.

- taking, accessing, using, manipulating, and/or disseminating photographs and/or videos without consent (including 'revenge pornography')
- sharing and/or disseminating private information and/or content, including (sexualised) images, audio clips and/or video clips, without knowledge or consent
- doxing (researching and broadcasting personally identifiable information about an individual without consent, sometimes with the intention of providing access to the woman in the 'real' world for harassment and/or other purposes)
- contacting and/or harassing a user's children, extended family, colleagues (etc) to gain access to her

39. *Surveillance and monitoring*

- monitoring, tracking and/or surveillance of online and offline activities
- using spyware or keyboard loggers without a user's consent
- using GPS or other geolocator software to track a woman's movements without consent
- stalking

40. *Damaging reputation and/or credibility*

- deleting, sending and/or manipulating emails and/or content without consent
- creating and sharing false personal data (like online accounts, advertisements, or social media accounts) with the intention of damaging (a) user's reputation
- manipulating and/or creating fake photographs and/or videos
- identity theft (e.g. pretending to be the person who created an image and posting or sharing it publicly)
- disseminating private (and/or culturally sensitive/ controversial) information for the purpose of damaging someone's reputation
- making offensive, disparaging and/or false online comments and/or postings that are intended to tarnish a person's reputation (including libel/ defamation)

41. *Harassment (which may be accompanied by offline harassment)*

- "cyber bullying" and/or repeated harassment through unwanted messages, attention and/or contact
- direct threats of violence, including threats of sexual and/or physical violence (e.g. threats like 'I am going to rape you')
- abusive comments
- unsolicited sending and/or receiving of sexually explicit materials

- incitement to physical violence
- hate speech, social media posts and/or mail; often targeted at gender and/or sexuality
- online content that portray women as sexual objects
- use of sexist and/or gendered comments or name-calling (e.g. use of terms like "bitch"/"slut")
- use of indecent or violent images to demean women
- abusing and/or shaming a woman for expressing views that are not normative, for disagreeing with people (often men) and also for refusing sexual advances
- counselling suicide or advocating femicide
- mobbing, including the selection of a target for bullying or harassment mobbing by a group of people rather than an individual and as a practice specifically facilitated by technology

42. *Direct threats and/or violence*

- trafficking of women through the use of technology, including use of technology for victim selection and preparation (planned sexual assault and/or femicide)
- sexualised blackmail and/or extortion
- theft of identity, money and/or property
- impersonation resulting in physical attack

43. *Targeted attacks to communities*

- cracking websites, social media and/or email accounts of organizations and communities with malicious intent
- surveillance and monitoring of activities by members in the community
- direct threats of violence to community members
- mobbing, specifically when selecting a target for bullying or harassment by a group of people, rather than an individual, and as a practice specifically facilitated by technology
- disclosure of anonymised information like address of shelters, etc.

C. UNDERLYING FACTORS AND ENABLING ENVIRONMENTS

44. As was also explored in the preceding sections, various factors – including cultural norms, socioeconomic status, the ordinary level of violence in the community concerned, the rate of Internet adoption and accessibility – play a role in creating negative enabling environments for online abuse and gender-related violence to flourish. These and other factors can also have a compounding effect on the impact of such abuse and violence, as well as the allocation and effectiveness of resources to ensure women gain access to justice and redress when they face such abuse and/or violence online.

45. Some of the key enabling factors discussed during the BPF are outlined below. Because these factors are of particular importance in contexts where women are either unconnected or only starting to gain access to the Internet and other technologies, the subsequent section (ii) investigates the underlying factors and considerations that are of relevance in creating positive enabling environments for women who are yet to gain Internet access.

i. Underlying factors

Lack of awareness, education, digital divide and digital literacy

46. A lack of awareness and recognition of online abuse and gender-based violence as abuse and/or violence was the factor that most survey respondents, for example, thought contribute to the incidence of online abuse and gender-based violence. Other related factors include a similar lack of awareness regarding available remedies and a lack of digital literacy and awareness of how to protect one's self from harm and how to be safe online.

47. In addition to a lack of awareness and low levels of digital literacy, there is also a tendency to trivialise or normalise online abuse and gender-based violence, particularly on social media platforms. This apparent trend, which is arguably related to a lack of awareness of the effects of online abuse and gender-based violence, is particularly harmful as it contributes to gender inequalities and a culture that may become increasingly hostile to female Internet users.

48. Digital divides often impact women in particular, with gender disparities being prevalent in both access to the Internet, as well as in terms of the skills of Internet users. These may be additional factors that contribute to the creation of enabling environments for abuse. Existing gender inequality in the field of ICT (discussed in next paragraph), as well as in economic, social and political dimensions, are related factors that impact whether women can participate online and what behaviour women experience online.

Gender inequalities

49. The ways in which inequality and sexism in offline environments, including gender norms, expectations and/or stereotypes, are reflected and amplified in online spaces are also important enabling factors for online abuse (for example stereotypes like 'women are not good in tech', 'girls cannot be gamers').

Example from Afghanistan:[47]
A BBC study shows how Afghan women face widespread online abuse including the unlawful distribution of naked pictures and the creation of fake accounts, particularly on Facebook. As a BPF contributor explains:

> *'These stories are examples of what actually happens with women online in Afghanistan. Men usually send friend-requests or inappropriate text messages to women they don't know. They are harassed when they post comments or publish their pictures. Their pictures are stolen and fake accounts are created to defame them or destroy their reputation in the society. Naked pictures or other forms of sexual material are transmitted to them which forces women to use aliases and take down their pictures or they shut down their social media accounts.'*

50. Discrimination against women in education in general, and gender gaps in academic disciplines of specifically science, technology, engineering and mathematics (STEM) in particular mean that fewer women and girls able to participate in fields relevant to the Internet and its governance. Women's unequal participation as decision makers in the development of technology platforms and policies is also an important factor; leading to the frequent neglect of issues that are of particular relevance and importance to women. Not only is technology furthermore predominantly viewed as 'masculine', but the technology industry also has significantly more men than women. Policy discussions around Internet governance furthermore tend to be dominated by male participants, and there are examples of technology-related harassment occurring during and after women's participation in Internet governance events.

51. Furthermore, multiple and overlapping forms of discrimination against women based on their race, ethnicity, caste, class, sexuality, disability, migrant and/or refugee status also permeate online environments, as can be seen from the sections above (see Section B iii) discussing the impact of online violence and gender-based violence in specific contexts.

Social norms/ cultures of violence and patriarchy

[47] Summarised from case study submitted by Said Marjan Zazai, National Information Technology Professionals Association of Afghanistan, Afghanistan. See Appendix 3, page 113. Media report on story available online (in Persian): BBC (15 August 2015). *Afghan Women on Facebook*. Available online: http://www.bbc.com/persian/afghanistan/2015/08/150823_k04_afg_women_problem_in_facebook?ocid=socialflow_facebook#share-tools). [Accessed 30 October 2015].

52. Closely related to the aforementioned factor of gender inequality, the existence of certain social norms and expectations in many societies leads to reluctance to report abuse. Not only are victims often blamed for the abuse they experience online, but they also feel that perpetrators will not be held accountable and that online actions are seemingly immune from the rule of law.

53. Victims/ survivors also often face social stigma and reputational risks in reporting online abuse, and technology-related abuse is still trivialised in many societies. There appears to be a related lack of recognition for the psychological and other harms of online abuse and/or gender-based violence, with victims/ survivors having limited or no recourse to relevant support systems.

54. Women may experience online abuse that is concurrent to and related with physical abuse and/or violence. Conflict within an intimate partner relationship or a woman's immediate circle of family members, friends and/or colleagues can contribute to the incidence of online abuse and violence; as well as emotional trauma like separation, divorce, and/or a history of rape, sexual and/or domestic abuse.

Legal and political context

55. For victims, a lack of support frequently extends to the legal and political environments they find themselves in. Authorities, including police officers, are sometimes unsympathetic, tend to lack relevant training in how to address online abuse and gender-based violence, and sometimes do not even have the necessary equipment (e.g. computers with Internet access) and technological skills or awareness for finding evidence of online abuse and gender-based violence. When victims do manage to have an incident reported and investigated by law enforcement officials, they face further difficulties in terms of the abilities and technological knowledge of mediators and/or the judiciary (including court systems, magistrates, judges, and other officers of law). For example, some judges faced with deciding a case about defamatory and abusive posts on a Facebook wall might struggle to understand the potential impact of such a form of abuse, and similarly, in making rulings and issuing judgments, tend to neglect the realities of how online posts are distributed on the Internet. The pace at which many cases can be investigated and heard, and the costs of judicial proceedings, are furthermore prohibitive for many victims.

56. In addition to potentially reluctant and indifferent law enforcement and judicial systems, legal and political environments in many countries make it even more difficult for victims/ survivors to institute complaints and cases. There is also a reluctance in some countries to extend existing definitions of abuse and gender-based violence (and the availability of related legal remedies) to cover online abuse and gender-based violence; and where new forms of abuse and violence

develop, there is a further lack of political will in some countries to enact laws and/or deal with it. In many countries there is a need to review existing legislation and policies and to determine how relevant they are for current realities in the context of online abuse and gender-based violence; whilst keeping in mind the need for flexibility to account for the pace of technological change.

57. Existing laws that address the violation of related rights (such as laws related to privacy, misuse of network systems and services, copyright and 'obscenity') and that are sometimes recommended for use to address online abuse and gender-based violence, neglect the gender-specificity of these acts, and fail to provide adequate redress to the harms that are faced. For example, obscenity laws that are used to criminalise sexual content often do not distinguish between consent and lack of consent in the creation and distribution of content. This can have the effect of criminalising consensual sexual expression of women, and can render both the victim and perpetrator as equally liable for the violation. In another example, women are sometimes forced to use problematic copyright laws to remove sexualised images of themselves that were published online without their consent. In addition to the cost and jurisdictional challenges of accessing these laws, victims/ survivors are also compelled to send the same images to relevant authorities to establish copyright ownership; extending the impact of the harm.

58. There are also existing challenges in addressing offline gender-based violence by authorities, with such violence often being regarded as 'less serious' than other forms of violence. Located within this phenomenon, online abuse and gender-based violence face an additional barrier for prioritisation by authorities to investigate and prosecute. Because the consequences of online abuse and gender-based violence are not as easily detected as offline violence, authorities tend to prioritise forms of offline abuse and/or violence with visible ‘effects’ on women and girls.

59. When cases are effectively brought before and adjudicated by courts and tribunals, existing legal remedies for criminal abuse and violence are often unsuitable for and ineffective in an online context as they fail to account for and adequately deal with the pace of technological change and the ways in which, for example, content is shared and distributed online. The inadequacy of mechanisms available on online platforms to enable effective responses to cases of online abuse and gender-based violence makes it even more difficult for victims/ survivors. For these reasons, women often feel that there are little or no consequences and a perceived impunity for online crime. There is therefore a need to review existing remedies and to, importantly, talk to the women and victims/ survivors involved to determine how suitable and useful existing remedies were and are to them.

60. Lastly, the cross-jurisdictional nature of the Internet means that authorities, including law enforcement or even Internet intermediaries like

telecommunication companies can find it difficult to investigate and pursue cases of online abuse and gender-based violence; reinforcing the importance of cooperation amongst national and international stakeholders.

Example from Britain:[48]
When a Muslim woman left her forced marriage, her ex-husband (who is not based in the UK) started setting up fake profiles for her on social media. He not only alleged that she is a prostitute, but also offered her services and shared her personal contact details. She was disowned by her family and received requests for her 'services'. While police are involved, little support has been offered because the woman's husband (the perpetrator) is outside the UK.

Example from Argentina:
After breaking up with her boyfriend, a woman found that several naked pictures and a sex tape of her were published without consent on a Facebook group that she shared with co-workers. The photos were also distributed on two porn websites (one based in Argentina and another in the USA). She reported the situation to Facebook, Google and other websites concerned, but did not receive a response. She then made a complaint at the Personal Data Protection Center for Buenos Aires Ombudsman's Office. Whilst the content was finally removed, it is still possible to access to some images from other websites that has republished the content from other jurisdiction.[49]

ii. Ensuring safe environments for future Internet users[50]

61. Technological advancement in connectivity has expanded broadband access and mobile penetration in recent years – also for women. But a gender digital gap still persists and is expressed in multiple dimensions. This begins from unequal access to basic Internet infrastructure; the affordability of connectivity costs and devices; gender disparity in education opportunities, including digital literacy; an uneven capacity to use the Internet for their needs and priorities; specific gender-based challenges and barriers, including the availability of relevant content and the censorship of online content related to gender and sexuality; and gender-based harassment and violence, both in physical spaces for accessing the Internet (such as public access points like cybercafes) and in online environments (including online harassment and cyberstalking).

---

[48] Summarised from case study submitted by Laura Higgins, SWGfL, UK. See Appendix 3, page 89.
[49] Example summarised from submission by Agustina Callegari, Personal Data Protection Center for Buenos Aires Ombudsman's Office, as part of comments on Draft II (submitted October 2015). See Appendix 4.
[50] *Policy Options for Connecting the Next Billion* is one of the themes that define the IGF's intersessional work in 2015. For this reason, the BPF decided to also consider issues related to access in relation to women and online abuse and gender-based violence. Read more here: IGF (2015). *Policy Options for Connecting the Next Billion.* Available online: http://www.intgovforum.org/cms/policy-options-for-connection-the-next-billion. [Accessed 30 October 2015].

62. While there are various ongoing processes aimed at improving connectivity – like the IGF's intersessional activity on the theme;[51] the ongoing process of reviewing progress made since the World Summit of the Information Society (WSIS+10); and the discussion of the post-2015 Sustainable Development Goals (SDGs) – it is crucial that these gaps are addressed. Addressing the issue of gender and access to the Internet requires an approach that is located within economic, social, political and cultural contexts. It is both short-sighted and inadequate to respond to this issue by looking at infrastructure or economic issues without examining the interplay of various other factors that act as pre-conditions as well as influencing factors to the extent that women and girls are able to access and use the Internet freely, safely and equally in the full exercise of their rights. This includes taking into consideration the impact of online abuse and gender-based violence as a barrier to access, as well as the creation of enabling environments for the protection of women's rights online in tandem with efforts to connect women to the Internet. Likewise, it is impossible to address online abuse and gender-based violence without also addressing the issue of gender digital disparities.

63. As with other broad public policy issues in Internet governance,[52] efforts to combat and address online abuse and gender-based violence often emanate from the developed world and also tend to reflect conditions, cultural perceptions and expectations in developed countries. On the other hand, addressing the problem is generally less of a priority in developing countries with lower levels of Internet penetration and access; where there may also be a lack of infrastructure, will and capacity to monitor, address and prevent online and offline abuse and violence. A potential way forward is to extend current definitions of abuse and gender-based violence to include the online dimension, which can then translate into the inclusion of online abuse and gender-based violence into the application and reform of existing anti-violence against women laws, the allocation of resources, and the development of policies and programmes.

64. While much can be learnt from the experiences of developed countries with high levels of Internet access and use, preconceptions of what constitutes 'best' practices to counter online abuse and gender-based violence cannot simply be extrapolated from developed countries for implementation in developing countries. As mentioned and investigated elsewhere in this report (see Section B iii and Section C i), different contexts have a significant impact on the nature of online abuse and mechanisms used to address online abuse and gender-based violence. There is thus a need for further research to study differences in context and to tailor programmes and mechanisms to specific local contexts.

---

[51] *Ibid.*

[52] See, for example: IGF (2014). *Best Practice Forum on Online Child Protection*. Available online: http://www.intgovforum.org/cms/documents/best-practice-forums/best-practices-for-online-child-protection/413-bpf-2014-outcome-document-online-child-protection/file. [Accessed 30 October 2015].

65. Many social media platforms used globally are located in developing countries, specifically in the USA, but have diverse regional, national and local impact. As such, greater attention needs to be paid by Internet intermediaries in thinking through responses that are also responsive to experiences in developing contexts.

66. Online abuse and gender-based violence also constantly evolve and may become increasingly sophisticated. It was interesting to note, for example, that many survey respondents felt that denying women access to the Internet or to certain online services is a worrying tendency particularly relevant as and when governments are working to connect the unconnected. Women may, for instance, be denied access to information and crucial support (including when, for example, governments in both developed and developing countries install filters to ostensibly address online pornography, but also act to over-filter and limit women's access to information about female health, reproduction and other issues).

67. Similarly, industry practices related to zero rating (including by oganizations like Google and Facebook) may negatively affect competition, access to the Internet and/or online content, and/or could interfere with end users' access to online information, including denying a specific segment (e.g. women) access to the developmental benefits that the Internet offer.[53] Zero-rated services may also have an impact on first-time Internet users' experience of online services and content; and influence their engagement and expectations. This is also linked to gender norms: for example, research[54] into gendered differences of social media tools like Facebook and WhatsApp in Pakistan indicated that women in Pakistan are much more likely to adopt WhatsApp and men are more fond of Facebook. The research seems to suggest that technologies can also reinforce and maintain existing social norms, with women preferring WhatsApp as a tool to reinforce and strengthen relations with family and friends while retaining their privacy, while men can be more 'public' on Facebook.

[53] Summarised from comment submitted by Zakir Syed, Pakistan, on Draft JP, using the BPF's public mailing list (submitted on 11 October 2015).

[54] Example submitted by Sadaf Baig, Media Matters, Pakistan. Article available at: Emrys Shoemaker, Tanqeed (July 2015). *Facebook Domestication.* Available online: http://www.tanqeed.org/2015/07/facebook-domestication/. [Accessed 30 October 2015].

D. BALANCING RIGHTS AND INTERESTS

i. Human rights and interests in online contexts

68. In addition to formal confirmations[55] that existing human rights instruments and guarantees apply equally online, there have been a number of initiatives to formalise a constitution and/or bill of rights for the Internet over the past few years (for example Brazil's Marco Civil da Internet,[56] the African Declaration on Internet Rights and Freedoms,[57] and Italy's Declaration of Internet Rights[58]); arguably indicating a growing recognition of the importance of ensuring that online spaces also adhere to offline perceptions of human rights protections and obligations.

69. However, the realisation and defence of the human rights of women is still an important and persistent challenge globally. The application of human rights standards needs to take into account the specificity of women's realities, including gender-based inequality and discrimination at economic, political, social and cultural spheres. As noted by the Office of the UN High Commissioner for Human Rights:[59]

> *'Effectively ensuring women's human rights requires, firstly, a comprehensive understanding of the social structures and power relations that frame not only laws and politics but also the economy, social dynamics and family and community life.'*

70. This extends to the online sphere, where disparity in access to ICTs, skills, literacy, decision-making and other contextual factors all act to affect the realisation of women's human rights online. In the balancing of rights and interests, these factors need to be taken into account.

ii. A balancing exercise?

---

[55] UNHRC (29 June 2012). *The Promotion, Protection and Enjoyment of Human Rights on the Internet* (A/HRC/20/L.13). Available online: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280. [Accessed 28 October 2015].
[56] Pensando O Direito (23 April 2014). *Marco Civil da Internet*. Available online (Portuguese): http://participacao.mj.gov.br/marcocivil/lei-no-12-965-de-23-abril-de-2014/. [Accessed 30 October 2015].
[57] [No author] (2014). *African Declaration on Internet Rights and Freedoms.* Available online: http://africaninternetrights.org/declaration-container/declaration/. [Accessed 30 October 2015].
[58] Committee on Internet Rights and Duties, Chamber of Deputies (August 2015). *Declaration of Internet Rights.* Available online: http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf. [Accessed 30 October 2015].
[59] UN Human rights (n.d.). *Women's Human Rights and Gender Equality* (webpage). Available online: http://www.ohchr.org/EN/Issues/Women/WRGS/Pages/WRGSIndex.aspx. [Accessed 2 November 2015].

71. Not only is no human right absolute, but different regions and/or countries tend to attach different weights of importance to different human rights around the world. In the USA, for example, freedom of expression carries particular significance that may result in other rights and freedoms facing potential limitation. Other countries, like France, for instance, opt to limit freedom of expression to protect citizens' rights and interests under national law, as seen in, for example, the case of *Yahoo v LICRA*, which involved the sale of Nazi-related memorabilia in France using auction services hosted on US servers.[60]

72. Tensions around multiple rights are often raised in discussions to address abuse of women and gendered violence against women online. Women's rights advocates have responded by stating that online violence in effect curtails women's right to freedom of expression, public participation and privacy by creating a hostile and unsafe online environment that can result in women withdrawing from online spaces.

73. Similarly, while anonymity and the protection of privacy may be vital for the exercise of freedom of expression online, including the right of women to access critical information and support services, these rights may also help to enable online abuse and gender-based violence by providing perpetrators with a cloak of invisibility and, thus, perceived impunity.

74. There is thus a need for measures that protect women online to consider, include and balance multiple rights including the right to safety, mobility, to participate in public life, freedom of expression, and privacy; and to take into account existing inequalities and discrimination which may affect how rights are protected and recognised. Such balancing exercises need to consider the importance, nature and extent of any limitation proposed and should opt for the least restrictive means to achieve that purpose. In this section a few of the potentially competing rights that are of particular relevance to online abuse and gender-based violence are briefly discussed.

Freedom of expression

75. Measures to address online abuse and gender-based violence, especially when it relates to drawing limits around content and expression, is sometimes seen as limiting the right to freedom of expression. However, the fact that online abuse and gender-based violence acts to impede women's right to freedom of expression by creating environments in which they do not feel safe to express themselves (see Section E below for consequences and impact) needs to be included in these debates. Many forms of online abuse, like gender-based hate speech, for example,

[60] E.g. *Yahoo Inc. v. LICRA* 433 F.3d 1199 (9th Cir. 2006). Available online: http://law.justia.com/cases/federal/appellate-courts/F3/433/1199/546158/. [Accessed 30 October 2015].

chill women's online interaction by compelling them to self-censor or refrain from using certain platforms where they might be susceptible to online abuse.

76. A 2015 report on the status of freedom of expression in Norway notes that hate speech "contributes to social exclusion and increased polarisation. Moreover, such speech intimidates people and deters them from speaking publicly; thus weakening democracy. Hate speech fans prejudice, creates fear and anxiety among the affected groups, and deprives people of dignity. Hate speech can therefore trigger discrimination and harassment and/or violence".[61] Viewed in the context of existing discrimination and inequality, gender-based hate speech can seriously affect women's rights to freedom of expression. The report further notes:[62]

> *'groups that are already exposed to other forms of discriminatory behaviour will experience being subjected to hate speech in public as more stressful than individuals and groups who, to little or no extent, are subjected to discriminatory behaviour. From such a perspective, efforts against hate speech will also be an important contribution to the fight against discrimination and for equality. Furthermore, by reducing the extent of hate speech, it will promote real freedom of expression for those who currently choose not to participate in public debate.'*

77. It is important to note that efforts to address content and expression that result in abuse and/or gender-based violence include both legal and non-legal measures, such as improving access, digital literacy, the creation of enabling environments for diverse expressions, as well as clear and specific delineations of legal and illegal gender-based hate speech.

Anonymity and encryption

> *"…all tools are subject to abuse, and that's certainly the case with respect to anonymity."*
>
> **David Kaye (UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression) during BPF session at IGF 2015**

[61] Equality and Anti-Discrimination Ombud's Report (2015). *Hate speech and hate crime.* Available online: http://www.genderit.org/sites/default/upload/hate_speech_and_hate_crime_v3_lr.pdf. [Accessed 2 November 2015].
[62] *Ibid*, page 16.

78. While freedom of expression activists tend to support the protection of and right to encryption online,[63] for example, anonymity – whilst useful in enabling people to exercise their right to freedom of expression online – also enables and protects perpetrators of online abuse.

> *"… online violence against women not only reproduces offline dynamics of gender-based oppression, but benefit from the very same conditions which make online spaces important (and potentially safe) to women, such as anonymity and interactivity."*
>
> **BPF survey respondent from Brazil**

79. Threats to privacy and the disclosure of personal information can subject particularly women of diverse sexualities and gender identities to significant threats and attacks, both online and offline. At the same time, perpetrators often use anonymous accounts in perpetuating abusive behaviour and violations online. This presents a challenging context for addressing the issue of online violations of women's rights whilst balancing other fundamental rights.

80. To address the issue, David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, noted during the BPF's session at IGF 2015 that the "default option" for technologies should be anonymity; followed by an investigation of the problems that anonymity may cause. As he also wrote in a report on the topic in May 2015:[64]

> *'Encryption and anonymity [...] provide individuals with a means to protect their privacy [...], and enabling [...] those persecuted because of their sexual orientation or gender identity [...] to exercise the rights to freedom of opinion and expression.'*

81. Company policies on anonymity and real name policies may contribute to the manifestation of online abuse and gender-based violence. For example, in one case a survivor of domestic violence managed to avoid her ex-husband for 20 years until Facebook's "real-name policy"[65] allowed her abuser to track her down. The

[63] E.g. Office of the High Commissioner for Human Rights (May 2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (A/HRC/29/32). Available online, along with other background resources: http://daccess-ods.un.org/TMP/668197.572231293.html.
[64] Office of the High Commissioner for Human Rights (May 2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (A/HRC/29/32). Available online, along with other background resources: http://daccess-ods.un.org/TMP/668197.572231293.html.
[65] Facebook Help Centre (2015). *What Names Are Allowed On Facebook?* Available online: https://www.facebook.com/help/112146705538576. [Accessed 30 October 2015].

policy has also led to abuse of transgender people online: as reported by a transgender user in a media report,[66] the policy has led to transgender users' profiles being reported in what is viewed as a form of bullying or harassment, often motivated by sexual aggression or homophobia (see paragraph 31 above).

[66] Lil Miss Hot Mess, The Guardian (3 June 2015). *Facebook's 'real name' policy hurts real people and creates a new digital divide*. Available online: http://www.theguardian.com/commentisfree/2015/jun/03/facebook-real-name-policy-hurts-people-creates-new-digital-divide. [Accessed 29 October 2015].

E. IMPACT AND CONSEQUENCES

82. The social and economic impact of online abuse and gender-based violence on not only individuals but also wider communities are influenced by a multiple factors, and can be difficult to measure. The potential impact of online abuse and violations on human rights is also increasingly stressed by international organizations, however. A few examples follow.

83. In mid-2013 the UN Working Group on Discrimination against women in law and practice included a specific reference to the Internet as 'a site of diverse forms of violence against women'. The Working Group expressed concern that for 'women who engage in public debate through the Internet, the risk of harassment is experienced online, for example, an anonymous negative campaign calling for the gang rape of a woman human rights defender, with racist abuse posted in her Wikipedia profile'. It also recommended that states support women's equal participation in political and public life through ICTs, including by ensuring gender-responsiveness in the promotion and protection of human rights on the Internet, and improving women's access to the global governance of ICTs.[67]

84. At the end of 2013, the UNGA adopted a consensus resolution[68] on protecting women human rights defenders with language on technology-related human rights violations:

> *'... information-technology-related violations, abuses and violence against women, including women human rights defenders, such as online harassment, cyberstalking, violation of privacy, censorship and hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights.'*

85. In 2015, furthermore, the UN Special Rapporteur on violence against women's report to the 29th session of the Human Rights Council on her mission to the UK, expressed concern about "women aged between 18 and 29 being at greatest risk of threatening and offensive advances on the Internet".[69]

---

[67] UNGA (19 April 2013). *Report of the Working Group on the issue of discrimination of women in law and practice* (A/HRC/23/50). Available online: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.50_EN.pdf. [Accessed 30 October 2015].

[68] UNGA (30 January 2014). *Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders* (A/RES/68/181). Available online: http://www.gender.cawater-info.net/publications/pdf/n1345031.pdf. [Accessed 30 October 2015].

[69] UNGA (19 May 2015). *Report of the Special Rapporteur on violence against women, its causes and consequences, Rashida Manjoo* (A/HRC/29/27/Add.2). Available online:

86. Despite the aforementioned examples, there is still a lack of awareness of and respect for women's rights and the impact of online abuse and gender-based violence on specifically women's rights (as is also indicated by the survey results[70]). This lack of awareness not only reinforces the importance of sensitisation, raising awareness and literacy programmes on the importance of women's rights, but it also makes it difficult for victims to make claims for the fulfilment and enforcement of such rights.[71]

87. Some of the common consequences of online abuse were identified from BPF participants' input, and through the broad stakeholder survey, and are outlined below.[72]

i. Impact on individuals

> *"[We need to]…recognise that the threats of online abuse directly attack freedom of the media and freedom of expression, because essentially women who have been abused [for example female journalists]… sometimes take themselves off social media. They may choose not to report on certain issues on certain topics because of the abuse that they have suffered. So that's leading to censorship."*
>
> **Frane Mareovic (Director Office of the OSCE Representative on Freedom of the Media, Bosnia and Herzegovina) during BPF session at IGF 2015**

88. Women commonly suffer fear, anxiety and depression as a result of online abuse and/or gender-based violence; reducing their involvement with the Internet and leading to their withdrawal from online spaces (sometimes to the extent that it may lead to suicide or attempted suicide). Victims' work, ambition and income are frequently affected; and they may experience their mobility being limited and/or curtailed.

---

http://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/AnnualReports.aspx. [Accessed 30 October 2015].

[70] For example, few respondents explicitly recognised that online abuse impacts women's rights, although respondents did list various other things that online abuse may impact. While the survey results are by no means representative of a larger population, the lack of importance that the respondents attached to online abuse as a limitation and violation of women's rights was noteworthy.

[71] See: CEDAW (23 July 2015). *General recommendation on women's access to justice* (C/CG/33). Available online: http://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_33_7767_E.pdf [Accessed 28 October 2015].

[72] This is, again, by no means an exhaustive list, but was compiled upon input from BPF participants.

Example from Suriname:[73]
A pilot study done in Suriname amongst a sample of young female Internet users indicated that respondents believe the effects of online abuse and gender-related violence to be serious. The contributor argues:

> *"It was very revealing that the majority of respondents felt that one of the consequences of online violence against women would be women/girls contemplating suicide or even acting on the thought of suicide. In most other cases the respondents felt that the women and girls would become depressive and may use the Internet less or not at all."*

89. Online abuse and/or violence is furthermore translated into offline environments when women experience their mobility being limited because of online abuse, including the disclosure of personal information online that carries the real threat of physical abuse and/or violence. It can also lead to the identification and/or preparation of victims for trafficking and/or other forms of offline abuse/violence.

ii. Impact on communities

> *"I have been online for just over 20 years, never in my life have I experienced the kind of abuse and harassment that has been following me around online for the past few years. It has made me stay offline, no longer engage in open conversations, become very distrustful of people generally, I've had problems sleeping, I've been afraid the individuals who have harassed me will turn up where I am in public..."*
>
> **anonymous BPF survey respondent**

90. One of the most common consequences of online abuse and gender-based violence on communities, according to survey respondents, is the creation of a society where women no longer feel safe online and/or offline. The problem also contributes to a culture of sexism and misogyny online and, in offline spaces, to existing gender inequality. In respect of the latter, online abuse and gender-based violence disadvantage women in limiting their ability to benefit from the same opportunities online that men frequently benefit from (e.g. employment, self-promotion and/or self-expression). See Appendix 5, in which attempts to attack the BPF's social media campaign are described, for examples of how online abuse impact communities.

[73] Summarised from case study submitted by Angelic del Castilho, Foundation Kinkajoe, Suriname. See Appendix 3, page 98.

F. SOLUTIONS, RESPONSES AND/OR STRATEGIES

91. Abuse and gender-based violence, whether perpetrated online or offline, is difficult to address because of the attitudes, stereotypes and beliefs that underpin it. In an online context, deciding upon appropriate measures to protect women is complicated because such measures need to be taken within the global context of the Internet with the cooperation of a multitude of stakeholders.

92. Efforts to develop, encourage and implement practices to counter online abuse and gender-based violence vary significantly around the world. The factors that contribute to the creation of environments that enable such behaviour also determine whether stakeholders will allocate resources to protect women's rights online, including existing gender inequalities, education systems, access gaps, digital literacy levels and the importance attached to encouraging gender equality, social and cultural norms in the country concerned, legal and political environments, and Internet adoption rates.

93. Due to the relatively recent recognition of this issue, the list of existing measures provided below is not an exhaustive list but is intended to be part of an increasing effort to document and collect emerging approaches. The aim is to provide snapshots of approaches as submitted by BPF participants, with the objective of potentially highlighting trends and lessons learnt that can inform future work. For this purpose, stakeholder groups were divided into government and public sector responses; multistakeholder and intergovernmental approaches; private sector responses; and community/ user-led approaches.

i. Public sector initiatives

94. While the scope of this BPF did not allow a detailed analysis of public sector approaches to the issue, various participants did submit examples useful to this work. General trends noticeable include that some countries have amended existing legislation to ensure applicability to online environments, whilst others have explicitly enacted new legislation to not only facilitate the aforementioned, but to also criminalise specific acts online and to ensure that intermediaries cooperate with authorities. Some examples of legislative initiatives in the public sector include:[74]

[74] Some of these examples are derived from: Carly Nyst, APC (May 2015). *End Violence: Women's Rights and Safety Online. Technology-related violence against women: recent legislative trends*. Available online: http://www.genderit.org/sites/default/upload/flowresearch_cnyst_legtrend_ln.pdf. [Accessed 30 October 2015].

Examples of public sector approaches

95. In **New Zealand**, the Harmful Digital Communications Act[75] was passed in July 2015. Initially introduced with the aim of addressing cyberbullying alone, the scope of the Act has since broadened significantly (and controversially) to target all content online that might be harmful. The Act not only amends existing legislation to ensure applicability to online spheres, but also creates an agency to which victims can turn when they face online abuse; a set of court orders that can be served against Internet hosts and authors upon referral by the aforementioned agency; new civil and criminal offences; and a 48-hour content takedown process whereby individuals can demand that online hosting providers remove content they believe is harmful.

96. In the **Philippines**, while there are various legislative instruments that indirectly and directly protect women's rights, it was only recently that policies and laws relating to ICTs are being put in place. This includes the controversial Anti Child Pornography Act, which has been criticised for potentially eroding Internet rights, the Anti-Photo and Video Voyeurism Act, and the Cybercrime Prevention Act (RA 10175). The latter includes a definition of 'cybersex', which was particularly criticised by women's rights groups and advocates for (among other reasons) its vagueness and broad scope, and for neglecting the underlying causes of online abuse and gender-based violence.[76]

97. In **Estonia**, a Strategy for Preventing Justice was approved in February 2015 and is currently being implemented by the Ministry of Justice.[77] Although online abuse and gender-based violence is not a separate topic in this strategy, measures to prevent cyberbullying, sexual offences online against children, and other forms of online abuse are reportedly being planned. Estonian courts enable victims of online abuse to apply for restraining orders in both civil and criminal proceedings; and the country is in the process of amending and adopting provisions relating to hate speech and to criminalise stalking.

98. While **Nepal** does not have any legislative provisions dealing directly with online abuse or violence, the Electronic Transaction Act[78] deals with cybercrime in general. The Act provides that the publication of illegal material online – specifically material prohibited by other legislation and that will be 'contrary to

[75] Parliamentary Counsel Office, New Zealand Legislation (2015). *Harmful Digital Communications Bill.* Available online: http://www.legislation.govt.nz/bill/government/2013/0168/latest/whole.html. [Accessed 30 October 2015].
[76] The position in the Philippines was summarised from a case study by Lisa Garcia, Foundation for Media Alternatives, Philippines. See Appendix 3, page 105.
[77] The Estonian position was summarised from a case study submitted by Piret Urb, Ministry of Foreign Affairs, Estonia. See Appendix 3, page 96.
[78] Nepal Law Commission (2008). *The Electronics Transaction Act, 2063.* Available online: http://lawcommission.gov.np/index.php?option=com_remository&Itemid=14&func=fileinfo&id=142&lang=en. [Accessed 30 October 2015].

the public morality or decent behavior' or that will 'spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities' may be liable to a fine or punishment.[79]

99. In the **United Kingdom**, one way in which the government has responded to the problem is by taking an information and support measure by launching a website, Stop Online Abuse,[80] in June 2015 to provide information, legal and practical advice to victims of online harassment, revenge porn, hate speech, sexual harassment and blackmail. The website is aimed at women, lesbian, gay, bisexual and transgender people after research found that they were most affected by the extreme cases of online abuse.

100. In **South Africa**, the Protection from Harassment Act[81] came into force on 27 April 2013; enabling individuals subject to online or offline harassment to apply to a competent court for a protection order lasting up to five years. The Act also contains provisions requiring electronic communications service providers to assist courts in identifying perpetrators responsible for harassment; and creates the offences of contravention of protection orders and failure of an electronic communications service provider to furnish required information. In March 2015, a draft Online Regulation Policy[82] was published with the objectives of (among other things) protecting children from exposure to disturbing or harmful material and premature exposure to adult material, and criminalising child pornography and the use and exposure of children to pornography. The draft regulations have been criticised[83] widely for its potential impact on online content and freedom of expression online, but also from the perspective of the practical impossibility of classifying all online content (including social media posts) before publication.

101. The Cyber-safety Act[84] of **Nova Scotia** (Canada) came into force in August 2013; enabling individuals subjected to cyberbullying (or, in the case of minors, their parents) to apply to a judicial officer for a protection order against an individual. The Act also contains provisions requiring electronic communications service providers to assist courts in identifying individuals responsible for

[79] Submitted as part of a case study submitted on the Nepali position by Shreedeep Rayamajhi, Nepal. See Appendix 3, page 114.
[80] Stop Online Abuse (n.d.) (website). Available: http://www.stoponlineabuse.org.uk/. [Accessed 31 October 2015].
[81] Government Gazette (5 December 2011). *Protection from Harassment Act, No. 17 of 2011*. Available online: http://www.justice.gov.za/legislation/acts/2011-017.pdf. [Accessed 30 October 2015].
[82] Government Gazette (10 March 2015). *Notice 182: Notice for Public Comment on Draft Online Regulation Policy.* Available online: http://www.fpb.org.za/profile-fpb/legislation1/514-draft-online-regulation-policy-2014/file. [Accessed 30 October 2015].
[83] Enrico Calandro, Research ICT Africa (2015). *The South African Draft Online Regulation Policy as a form of "censorship by proxy".* Available online: http://www.researchictafrica.net/home.php?h=155. [Accessed 30 October 2015].
[84] NS Legislature (2013). *Bill No. 61*, *Cyber-safety Act*. Available online: http://nslegislature.ca/legc/bills/61st_5th/1st_read/b061.htm. [Accessed 30 October 2015].

cyberbullying, and creates the tort of cyberbullying, which enables individuals to sue others for damages arising out of cyberbullying.

102. In the **USA**, in the state of California, the controversial SB 255 Electronic Communication Devices: Prohibited Distribution of Personal Information Act[85] came into effect in October 2013 and creates a new misdemeanour of disorderly conduct by way of distribution of intimate photographs with the intent to cause serious emotional distress. The Act is narrowly worded and focuses on instances in which the person who takes or makes the intimate image, distributes it with the intent to cause, and the effect of causing, serious emotional distress to a victim. It has been criticised for potentially criminalising speech and allowing prosecution in victimless instances. In Arizona, the Arizona Revised Statute 13-1425 was passed in 2014 with the objective of preventing revenge pornography, but with far broader implications. In a recent case, *Antigone Books v. Brnovich*,[86] the plaintiffs argued that the law amounted to the unconstitutional limitation of free speech by criminalising more than only offensive actions. In accordance with the court order, prosecutors in the state were ordered to halt the enforcement of the law.

Challenges and ideas for further exploration:

103. There is a need for public sector initiatives to acknowledge and recognise that although online abuse and gender-based violence might not cause physical harm in all instances, it can cause significant emotional and psychological harm, as well as impact on issues such as mobility, employment and public participation (see Section E above for a more thorough exploration of consequences and impact). These are equally important factors to address and prevent.

104. As a key priority, public sector initiatives need to address the underlying causes that contribute to and enable online abuse and gender-based violence (as discussed in Section C i above) – specifically existing gender inequalities. Without addressing root problems, public sector intiatives tend to adopt merely reactive stances to incidents. Citizen support is also easier to facilitate when the public sector invests in public education to address the underlying causes that contribute to and enable online abuse and gender-based violence. The UK government's anti-trolling website (see paragraph 99 above) can arguably be seen as one such way forward. There is also a related need to invest in research and statistics (and proper reporting guidelines) to be able to study the incidence of online abuse and gender-based violence.

---

[85] LegiScan (2015). *California Senate Bill 255*. Available online: https://legiscan.com/CA/text/SB255/2013. [Accessed 30 October 2015].
[86] District Court for the District of Arizona (10 July 2015). *Antigone Books LLC et al v State of Arizona*. Order available online:
https://www.aclu.org/sites/default/files/field_document/antigone_v_horne_final_decree.pdf. [Accessed 30 October 2015].

105. In terms of responses, governments and the public sector tend to favour legislative instruments, which often take a lot of time to be developed and adopted. While these due processes generally allow for beneficial public consultation (when legislative instruments are not unduly rushed), the pace at which Internet platforms develop, including the ways in which online abuse of women also evolve and change, often reduce the efficacy of such legislative responses by the time it is actually adopted. Some countries also tend to utilise and amend existing legal frameworks rather than creating new laws specifically for new technologies (e.g. South Africa, paragraph 100 above). Not only does the adequacy of this approach for providing redress need to be investigated, but the public sector also needs to consider flexible and potentially informal measures for responding to online abuse and gender-based violence, although such measures need to be transparent at all times. To read more about the challenges and efficacies of efforts in the UK to address the distribution and viewing of child abuse images online, including the tendency of such filters to also block legitimate online content, see Freedom House's *Freedom on the Net* (UK edition) report.[87]

106. Governments should also ensure that they facilitate and simplify access to justice for survivors[88] whilst prioritising redress and relief over criminalisation. Where possible, governments should consider options beside traditional courts and tribunals. The creation of specialised, fast-track courts or specialised agencies to investigate complaints can, for instance, help to provide simple, quicker and more cost-effective (especially in comparison to ordinary courts) forms of recourse to victims. Where possible, such agencies should be able to accept third party complaints and should be able to act both reactively, in response to specific complaints, and proactively in response to potential trends and/or cases of online abuse and/or gender-based violence. In Estonia, for instance, specialised police officers[89] give advice regarding online crimes and also refer cases to police stations when necessary, while in Canada a cyberbullying investigative unit[90] provides an easy process for individuals to make complaints.

107. While the effectiveness of protection orders in the context of online abuse and/or gender-based violence remains to be seen, these orders are already used in many countries to address domestic violence by providing a practical means of halting violence without requiring victims to become embroiled in lengthy and demanding criminal processes.

---

[87] See Freedom House (2015). *Freedom on the Net 2014* (UK). Available online: https://freedomhouse.org/report/freedom-net/2014/united-kingdom. [Accessed 30 October 2015].
[88] See: CEDAW (23 July 2015). *General recommendation on women's access to justice* (C/CG/33). Available online: http://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_33_7767_E.pdf [Accessed 28 October 2015].
[89] Politsei- ja Piirivalveamet (30 October 2015). *Web Constables give advice on the Internet.* Available online: https://www.politsei.ee/en/nouanded/veebikonstaablid/. [Accessed 30 October 2015].
[90] Cyberscan (n.d.) (website). Available online: http://cyberscan.novascotia.ca/#second_white. [Accessed 30 October 2015].

108. Before introducing legislative instruments or amendments, the public sector needs to consult citizens and victims to first determine their needs. This includes women's rights organizations in order to integrate a gendered awareness into potential measures to avoid a further potentially discriminatory effect (e.g. Philippines, paragraph 96 above). When legislative instruments are required, proper consultation processes (including opportunities for public comment on legislative designs) also need to be followed to ensure citizen support. The public sector should not only respond reactively to high profile cases of abuse by rushing through legislative instruments with limited consultation.

109. The public sector also needs to explore its legal relationship with Internet intermediaries and the level of obligations it can realistically impose on intermediaries. Some countries have already passed and amended legislation to compel electronic service providers to provide information to courts in certain instances of abuse (e.g. Nova Scotia and South Africa). While intermediaries may have certain obligations to help prevent and rectify online abuse and gender-based violence that occurs on their platforms, any duties imposed upon them arguably need to be both flexible, to account for technological change, and workable, to account for the nature and speed of content distribution. While the responsibility of educating users and improving digital literacy levels arguably lies primarily with the public sector, governments should consider cooperating with intermediaries to ensure education also continues on the platforms. Where new users join a social media platform, for instance, they could be required to first complete a simple and engaging online training programme that interactively teaches users about user rights and duties, how to respect other users, what kind of behaviour will not be tolerated, and how to easily report abuse, for instance.

110. Tensions that arise when questions of multiple rights and interests are concerned, as described in Section D above, is vital in public sector approaches. New legislation has sometimes differentiated between online and offline communication and expression that might have the good intention of protecting users online, but that introduce the potential for damaging freedom of expression (e.g. New Zealand, paragraph 95 above). While it might be useful for legislative instruments to recognise the unique nature of digital communication and the nature of harm attributed to online speech, in light of the speed of proliferation, the current inability to permanently erase content, and the anonymous nature of some online content, if legislation enables courts to have too much judicial discretion for interpretation, such legislation might be applied in ways that could limit free expression and could undermine the free flow of information.

111. In cases where private information or content like photographs and videos are distributed without consent, laws related to online defamation, voyerism and the wilful exposure of private and/or intimate material are sometimes used. However, in most jurisdictions, an accused can defend him/ herself by arguing that the

content was true and in the public interest. This defence can expose the victim to more emotional trauma in the process of establishing 'truth', while definitions of the 'public interest' are highly dependent on the society concerned (see Section B above for more on the importance of contexts and enabling environments). An arguably better approach could be a stronger application of the right to privacy online and offline, that takes into consideration existing gender disparity and discrimination.

ii. Multistakeholder and intergovernmental initiatives

112. Due to increasing recognition of the importance to develop practices to counter online abuse and gender-based violence, there have been some initiatives taken by various intergovernmental agencies and multistakeholder approaches to address the issue.

113. The **Council of Europe**'s Convention on Preventing and Combating Violence against Women and Domestic Violence,[91] which entered into force in August 2014, places particular emphasis on the role of the ICT sector and the media in preventing violence targeted at women. Media organizations are encouraged to introduce self-regulatory mechanisms, internal codes of conduct/ethics and internal supervision measures to promote gender equality, to combat gender stereotypes, to avoid sexist advertising, language and content, and to refrain from the use of degrading images of women associating violence and sex. State parties are furthermore encouraged to cooperate with the private sector to equip children, parents and educators with the necessary skills for dealing with the ICT environments that provide access to degrading content of a sexual or violent nature.[92] Monitoring mechanisms are currently being put into place and the first evaluations are expected in 2016.[93]

114. The **Broadband Commission** for Sustainable Development, an initiative steered by UNESCO and the ITU, was established in May 2010 with the aim of boosting the importance of broadband on the international policy agenda. In September 2015, a report by its Working Group on Broadband and Gender (co-chaired by UNDP and UN Women) was released. The September report critiques the volume of 'cyber violence' against women and girls and its social and economic implications for women online, and also highlights law enforcement agencies and courts' failure to take 'appropriate' action to counter the problem. It argues that whilst legal and social approaches on a national level is challenging because of the global

[91] Hereafter 'the Istanbul Convention', which has been signed by 20 member states and ratified by 18 member states. Available: Council of Europe (2014). *Convention on Preventing and Combating Violence Against Women and Domestic Violence.* Available online: http://conventions.coe.int/Treaty/EN/Treaties/Html/210.htm. [Accessed 30 October 2015].
[92] See Article 17 (*ibid*).
[93] The Council of Europe's position was summarised from a case study submitted by Bridget O'Loughlin, Council of Europe. See Appendix 3, page 102.

nature of the Internet, 'rigorous oversight and enforcement of rules banning cyber violence' is 'an essential foundation stone' for a safe Internet. It proposes a three-pronged approach of cyber violence abuse and gender-based violence, along with a controversial and problematic recommendation calling for political and governmental bodies to 'use their licensing prerogative' to force 'Telecoms and search engines' to 'supervise content and its dissemination'. Following criticism, the report was withdrawn in October 2015 and will be republished once 'relevant inputs have been taken onboard'. [94]

Challenges and ideas for further exploration:

115. These initiatives signal an increased recognition of the importance of engaging and identifying the roles that different stakeholders can play in understanding and responding to this issue at regional and global levels. This BPF is one such measure; demonstrating commitment also by the IGF community as a multistakeholder platform to facilitate such policy discussions. Further dialogue, monitoring and assessment of these initiatives will provide important lessons learnt for other initiatives to emerge.

116. As noted in earlier sections, however, measures need to be understood and located within a strong understanding of the interplay of social, cultural, economic and political structures and how these factors impact on online abuse and gender-based violence, as well the nuanced need to balance competing rights and interests.

iii. Private sector approaches

117. Some examples of private sector initiatives aimed at addressing online abuse and gender-based violence include:

118. **Twitter**'s abusive behavior policy[95] is aimed at evaluating and addressing potentially abusive behaviour on the platform if it is in violation of the Twitter Rules[96] and Terms of Service.[97] Twitter defines abusive behaviour as including (indirect or direct) violent threats; abuse and harassment; protecting users from self-harm; preventing anyone from publishing private information belonging to another; and impersonating others with the aim of misleading, confusing or

[94] Broadband Commission (2015). *Cyber Violence against Women and Girls: A world-wide wake-up call* (2015). Notice regarding retraction of report available online: http://www.broadbandcommission.org/Documents/reports/bb-wg-gender-report2015.pdf. As at 30 October 2015, the report remained available online at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259. [Accessed 29 October 2015].
[95] Twitter (n.d.). *Abusive Behaviour Policy.* Available online: https://support.twitter.com/articles/20169997#. [Accessed 31 October 2015].
[96] Twitter (n.d.). *The Twitter Rules.* Available online: https://support.twitter.com/articles/20169997#. [Accessed 31 October 2015].
[97] Twitter (18 May 2015). *Twitter Rules and Terms of Service.* Available online: https://twitter.com/tos?lang=en. [Accessed 31 October 2015].

deceiving others. It has a lighter touch approach to offensive content and mediation, which is tolerated as long as it does not violate the Twitter Rules and Terms of Service. It explains:

> *"Twitter provides a global communication platform which encompasses a variety of users with different voices, ideas and perspectives. Because of this diversity, you may encounter content you consider to be inflammatory or inappropriate that is not considered a violation of our rules."*

119. Twitter enables users to report violations[98] and receives complaints or reports from both individuals that experience abuse and third party complaints.[99] It has also changed its privacy rules from making tweets available for only 30 days to making all tweets since Twitter was created available and searchable on their website; which is helpful in collecting evidence in past cases of online harassment.

120. In March 2015, Twitter also introduced a change that makes it easier for users to report threats that they felt may warrant attention from law enforcement. When filing a report regarding a threatening tweet, the complainant has the option to receive a summary of their report via email. Clicking the "Email report" button sends the complainant an email that packages the threatening tweet and URL, responsible Twitter username and URL, a timestamp, as well as the complainant's account information and the timestamp of the report. Twitter's guidelines for law enforcement are also included in the report, including an explanation of what additional information Twitter has and how authorities are able to request it.[100] In addition, structures of single points of contact (SPOCs) in law enforcement, which have been implemented in countries like the UK, may make it easier for members of the public and Internet companies to react to online abuse and violence.[101]

121. **Facebook**'s Community Standards[102] were developed with the aim of helping users feel safer online. In terms of these standards Facebook's content reviewers can remove content, disable accounts and work with law enforcement agencies when it perceives a 'genuine risk of physical harm or direct threats to public safety'. It also allows personal and third party reports/ complaints, and specifically mentions that when governments request the removal of content that violate local laws but not Facebook's Community Standards, it may make such content unavailable in the relevant country or territory. Similar to Twitter, Facebook also stresses that 'because of the diversity of our global community,

---

[98] Twitter (n.d.). *How to report violations.* Available online: https://support.twitter.com/articles/15789#. [Accessed 31 October 2015].
[99] Twitter (n.d.). *Helping a friend or family member with online abuse.* Available online: https://support.twitter.com/articles/20170516#. [Accessed 31 October 2015].
[100] Twitter's measures were summarised from a submission by Patricia Cartes, Twitter. Submitted via email as comment on Draft II (October 2015). See Appendix 4.
[101] *Ibid.*
[102] Facebook (n.d.) *Community standards.* Available online: https://www.facebook.com/communitystandards. [Accessed 31 October 2015].

please bear in mind that something that may be disagreeable or disturbing to you may not violate our Community Standards'.

122. **Google** similarly acknowledges[103] that its services 'enable people from diverse backgrounds' to communicate and 'form new communities'. It has specific provisions related to harassment, bullying and threats, sexually explicit material, violence, and impersonation. A policy advisor at Google, Hibah Hussein, explained during the BPF's session at IGF 2015 that while Google tries to develop tools that make reporting easy and intuitive, it largely relies on users to "flag" content that might be illegal or harmful. She also noted the difficulty in deciding what content is harmful, violent and/ or abusive, stressing that a one-size-fits-all solution is not workable:

> *"We have… heard loud and clear from civil society groups and other actors that you don't really want an intermediary to make blanket decisions about what qualifies as harassment."*

Challenges and ideas for further exploration:

123. Company policies on anonymity and real name policies may contribute to the manifestation of online abuse and gender-based violence, as is explored in more detail in Section D ii above. In addition, the use of proxy accounts can also circumvent these requirements by sending automated harassment messages without being able to determine who the 'real' account holder is.

124. In formulating content regulation and privacy policies, intermediaries often fail to consider relevant social and other contexts; particularly in regards to online abuse of women and gender-related violence. Many policies reflect limited engagement with the perspectives of users outside North America or Europe, and reporting mechanisms and policies tend to be in English, which makes it difficult for non-English speakers to access and benefit from. Urdu, for instance, is often largely written in a 'Roman' format online – i.e. Urdu speakers use the English alphabet to phonetically spell out Urdu words; making it difficult for translation software to decipher real meanings. If a user wants to complain about something written in 'Roman' Urdu on Facebook, for example, Facebook would need an employee to translate in order to determine the real meaning of posts. In effect, this situation leads to harassment not being recognised as harassment unless it is written in the actual Urdu alphabet, which is easier for Facebook to translate.[104]

125. While many intermediaries do have terms of service and other user guides of conduct, some of these displays a reluctance to provide public commitments to human rights standards – something that might be understandable considering

[103] Google (n.d.) *User Content and Conduct Policy.* Available online: https://www.google.com/intl/en US/+/policy/content.html. [Accessed 30 November 2015].

[104] Example submitted by Sadaf Baig, Media Matters, Pakistan.

the number of countries with diverse 'beliefs' they hope to operate in. For this reason, however, many terms of service tend to become mere reflections of minimum legal obligations (e.g. copyright infringement and child exploitation), or focus primarily on freedom of expression. Terms of service also often lack definitions of what conduct actually amounts to unlawful and abusive behaviour; particularly forms of online gender-based violence and abuse, and tend to define the remedies available for victims/ survivors poorly.

126. Internet intermediaries can explore a clearer and more explicit commitment to more comprehensive human rights standards to better address the issue of online abuse and gender-based violence that takes place through, or in their services and platforms. The UN Special Representative on the issue of human rights and transnational corporations and other business enterprises compiled a set of *Guiding Principles on Business and Human Rights*, which was endorsed by the UN Human Rights Council in 2011.[105] The Guiding Principles, also known as the "Ruggie Framework", can provide guidance to Internet intermediaries on the actions they can take to ensure that women's rights online are promoted and respected in compliance with international human rights standards.

127. Some intermediaries do not have formal record-keeping systems and clear communication guidelines, and also lack the ability or will to remove individual content across the system at its source (e.g. when it comes to rape photos and videos being uploaded and spread virally, metadata should enable companies to track and locate content across its entire platform). Intermediaries also sometimes display a lack of transparency around reporting and redress procedures (see paragraph 141 below with regards to intermediary responsibility and transparency measures). In many of the case studies submitted to the BPF, for example, women reported that when they submitted complaints or concerns to an intermediary, they received either an automated or a complete lack of response. It was also noted by another commentator that Twitter's abuse policy, for instance, tends to be subjective and abused by users. The submission of a significant number of abuse reports by a small group of organized people may, for example, lead to the suspension of accounts without a clear violation being present.[106]

128. There are also challenges regarding the adequacy of available remedies offered by intermediaries. Multiple-strike policies are generally limited to copyright concerns and not to other violations like online abuse and gender-related violence (e.g. reserve the right to terminate accounts specifically on the basis of repeated gender-based harassment, hate and abuse); and the effectiveness of actual take-down procedures at certain sites remains unknown despite the likelihood of such

[105] UNHRC (2011). *Guiding Principles on Business and Human Rights.* Available online: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. [Accessed 2 November 2015].
[106] Example summarised from submission by J. Carl Henderson as part of submissions to Draft II (October 2015). See Appendix 4.

a platform being used to distribute videos and photos taken without consent of the people featured.

129. Lastly, intermediaries do not seem to invest enough in the promotion of user and staff literacy on the issue of online abuse and gender-related violence. Users are often unaware of their rights and responsibilities in online contexts, and intermediary staff similarly do not receive appropriate training to adequately address and deal with online abuse and gender-related violence.

iv. Community-led initiatives

130. A range of commercial and non-commercial civil society organizations, users and communities has made significant contributions to the address online abuse and gender-based violence, particularly as many of these have a global scope.

131. These initiatives have diverse objectives, including raising awareness about how to support victims; promoting digital safety education; enabling crowd-sourced blocking; identifying ('naming and shaming') perpetrators; encouraging public debates to promote norm-setting on online behaviour; and direct interventions in response to active (or real) cases of online abuse and/or gender-based violence. While it is impossible to highlight and describe each of these here, a few examples of these initiatives include:

Digital safety education and resources

132. Security-in-a-box,[107] which was created in 2009 by Tactical Tech and Front Line, aims to assist human rights defenders with their digital security and privacy needs by providing them with a collection of hands-on guides.

133. The Boston Safety Hub Collective's A DIY Guide to Feminist Cybersecurity[108] also provides an introduction to available cybersecurity tools, and manages a hashtag on Twitter (#SafeHubTech) to which users can also tweet cybersecurity questions and concerns.

Campaigns/ raising awareness

134. The APC's Take Back the Tech![109] campaign was launched in 2006 with the aim of encouraging the use of any ICT platform to promote activism against gender-based violence. It plans various campaigns throughout the year, with the biggest

[107] Tactical Technology Collective (2009. *Security in-a-box.* Available online: https://tacticaltech.org/projects/security-box. [Accessed 31 October 2015].
[108] A DIY Guide to Feminist Cybersecurity (n.d.) (website). Available: https://tech.safehubcollective.org/cybersecurity/. [Accessed 31 October 2015].
[109] Take back the tech! (n.d.) (website). Available: https://www.takebackthetech.net/. [Accessed 31 October 2015].

being 16 Days of Activism Against Gender-Based Violence (November 25 – December 10 each year).

135. Peng! is a collective that specialises in so-called 'subversive direct action, culture jamming, civil disobedience and guerrilla communications' launched its Zero Trollerance campaign[110] in March 2015. The campaign used Twitter profiles controlled by computer programs (or bots) to target suspected trolls and to troll them back with the aim of educating these alleged trolls. 5000 suspected trolls were identified with 'simple language analysis' of Twitter data tweeting 'the type of dangerous language often used to harass and incite violence against women and trans people'. While the campaign is controversial for using similar tactics as the trolls it targets, it raises interesting questions on counter-strategies that are responsive to context and the potential limits of such strategies.

136. End Online Misogyny[111] has created accounts on various social media platforms (including Twitter, Facebook, Pinterest and Tumblr) with the aim of highlighting and eradicating online misogyny and abuse by sharing real examples of misogynistic abuse from different users.

Helplines

137. Various helplines aim to assist women who face online abuse. In the UK, some of these helplines are supported by the UK Government Equalities Office in what appears to be a very useful public-private partnership.

138. The Revenge Pornography Helpline,[112] for example, was created as a pilot project in February 2015 with the objectives of supporting victims, assisting in the removal of harmful content, and collecting numeric data and evidence on online abuse and gender-related violence. The helpline works both reactively (in response to complaints from victims) and proactively by reporting and requesting the removal of abusive content.[113] The Professionals Online Safety Helpline,[114] in turn, was co-funded by the European Commission with the aim of supporting professionals working with children and young people in the UK with any online safety issues they may face themselves or with children in their care. The helpline provides support with all aspects of digital and online issues on social networking sites, including cyberbullying, sexting, online gaming and child protection online.[115]

---

[110] Zero Trollance (2015) (website). Available: https://zerotrollerance.guru/. [Accessed 31 October 2015].
[111] End Online Misogyny (n.d.) (website). Available: http://www.endmisogyny.org/. [Accessed 31 October 2015].
[112] Revenge Pornography Helpline (2015) (website). Available: http://revengepornhelpline.org.uk/. [Accessed 31 October 2015].
[113] Summarised from case study submitted by Laura Higgins, SWGfL, UK. See Appendix 3, page 89.
[114] UK Safer Internet Centre (n.d.). *Helpline.* Available online: http://www.saferinternet.org.uk/about/helpline. [Accessed 31 October 2015].
[115] Summarised from case study submitted by Laura Higgins, SWGfL, UK. See Appendix 3, page 89.

139. Both of these helplines maintain strong relationships with companies like Google, Yahoo, Microsoft, Twitter, Facebook, Snapchat and Tumblr. These relationships tend to be reciprocal, with the helplines providing the platforms advisory support on beta testing of new products or services, while platforms keep the helplines abreast of safety and reporting updates.[116]

Technical solutions

140. The development of certain applications aimed to help protect women in a variety of ways are also noteworthy, including certain tracking, monitoring and reporting mechanisms. HarassMap,[117] for instance, is used in Egypt with the aim of preventing sexual harassment both through online and mobile reporting and mapping and through media campaigns. Crowd-sourced maps are used to illustrate the scale of the problem and to raise awareness about the problem of sexual harassment.

Other responses

141. The Ranking Digital Rights[118] project was developed in recognition of the importance of Internet and telecommunication companies' responsibility to respect human rights online. While the project does not have a specific indicator targeted at measuring how companies deal with online abuse and gender-based violence, its 31 indicators are targeted at measuring how certain companies protect and uphold rights to privacy and freedom of expression, including how transparent and thorough they are in their reporting of content removal practices. As the project director, Rebecca McKinnon, noted at the BPF's session at IGF 2015, very few companies are transparent when the takedown of content is concerned, and there is a lack of accountability and stakeholder engagement and/ or awareness in this regard. She also stressed the difficulty of imposing blanket intermediary responsibilities:

> *"…the law is placing strong legal responsibility on platforms to police content, it always leads to over censorship. I'm not aware of any case where the censorship or the restrictions are done in a very sensitive way that only deals with real harassment and don't end up leading to the censorship of activists and take down accounts of people who have a right to be speaking and who are engaging in legitimate speech and women who are trying to get their message out."*

---

[116] *Ibid*.
[117] HarassMap (n.d.) (website). Available: http://harassmap.org/en/. [Accessed 31 October 2015].
[118] Ranking Digital Rights (n.d.) (website). Available: https://rankingdigitalrights.org/. [Accessed 29 November 2015].

G. CONCLUSIONS

142. The work of this BPF illustrates that whilst the issue of online abuse of women and gender-based violence is a complex, multi-dimensional one with no simple solutions, it is vital that it be addressed by all stakeholders in the Internet governance field and beyond. While the ongoing, open and iterative work of this BPF's multistakeholder community is aimed to be one step in this direction, much more work needs to be done to understand and address the issue of online abuse and gender-based violence.

143. Broadly speaking, the BPF's work illustrated the benefits of having a neutral platform where multiple stakeholders could contribute in order to address the issue in an open, transparent and inclusive manner using a mixed methodology that enabled a diversity of rich responses and input at various different stages of the BPF's work. At the same time, some experiences during the process emphasized the importance of balancing transparency with the need for a safe working and discussion environment for participants, particularly when difficult and contentious public policy issues like the current one are involved (see Appendix 5).

144. In the section below, the BPF's main recommendations and lessons are divided into first understanding the issue and then the considerations that need to be kept in mind in responding to the issue; followed by some additional considerations for future research:

i. Understanding the issue

A more comprehensive definition

> *"I think it's really important for us to have definitions of the problem that don't over regulate, because very often the tools that we would want to use in order to counter harassment will be the same tools that are used to censor…"*
>
> **David Kaye (UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression) during BPF session at IGF 2015**

145. The complexity of the issue starts with the definition. Whilst some BPF stakeholders called for clearer definitions to prevent abuse and the violation of rights, the BPF's work showed that the issue is not only interpreted and approached differently in diverse regions, but also that the terminology used for it is inconsistent, and that the nature and pace of technological development,

especially online, demand flexibility in defining related issues. Further, there was a range of acts that fell within the ambit of online abuse and gender-based violence. Greater clarity with regards to definitions, in particular ones that can comprehensively and clearly encapsulate its range and need for flexibility, could go a long way to helping advocates address the issue. A starting point could be linking them to, and expanding the manifestation of existing and recognisable forms of gender-based violence, and identifying new areas that are specific to ICTs.

146. The importance of comprehensive and flexible definitions is also evident when investigating the impact of diverse contexts and environments on online abuse and gender-based violence. This is why it is vital that further research study differences in context. Responses, programmes and mechanisms aimed at addressing the issue cannot be developed in a vacuum and need to similarly address specificity in contexts, whilst recognising the broader framework of online abuse and gender-based violence as an issue of gender-based discrimination and a violation of women's human rights.

147. The BPF also found that the issue must be studied whilst keeping offline environments, and potential repercussions (including physical, emotional and psychological harm) in offline/physical environments, in mind. Online violence and gender-based violence often compete with other forms of violence against women in priority agendas, making it important that definitions of abuse of and violence against women take clear cognisance of online forms of abuse and/or violence against women.

148. The need to understand and address the underlying causes that contribute to and enable online abuse and gender-based violence – specifically existing gender inequalities – is also of critical importance in ensuring a more comprehensive understanding the issue. One component of this is the consideration of gender disparities in access to, development of and decision making over ICTs.

Awareness, awareness, awareness

149. A lack of awareness about women's rights and the impact of the issue on individuals and communities contribute to an inability to make claims for the fulfilment and enforcement of such rights, and also reinforces the need for awareness, literacy and education programmes, along with more investment in research and statistics on the issue.

> *"I'm glad to hear that there's some research and data being collected about this because… but we need more data and understanding of the effects of the abuse, but also the sources of the abuse."*
>
> **Frane Mareovic (Director Office of the OSCE Representative on Freedom of the Media, Bosnia and Herzegovina) during BPF session at IGF 2015**

Calling for a better understanding of the rights and interests involved

150. Whilst the fact that 'offline' human rights apply equally online is widely recognised, there appears to be a discordance when the related obligations on stakeholders to protect and uphold these rights are called for where online abuse of women and gender-based violence are concerned.

151. There is also a need for further study and clarification on questions of multiple rights and interests, especially where freedom of expression, privacy and anonymity are involved; as well as on the often inadvertent consequences of company policies (e.g. real-name policies) on the manifestation of online abuse and gender-based violence. Emerging areas of policy work around delineating hate speech online, as well as the right to privacy in the digital age offer opportunities to expand this issue.

ii. Considerations in developing responses

152. In developing approaches to address the issue of online abuse and gender-based violence, the BPF found that many stakeholders' responses appear to be implemented without proper consultation with users. It is vital that public and private sector approaches to the issue be developed transparently in due consultation with current users (including victims and survivors of online abuse and/or violence), and also whilst considering the needs of future users as Internet access and adoption expand globally.

153. Many strategies also fail to consider the potential impact of certain approaches on other rights, making a better understanding of the rights and interests involved in addressing the issue (discussed above) vital. Consultation with civil society organizations working on human rights, women's rights as well as violence against women is an important measure for this consideration.

154. Where countries consider developing legislative responses to the issue, it is critical that remedy and redress be prioritised over criminalisation. Flexible and informal measures that can more easily, quickly and effectively respond to online behaviour need to be considered, although such measures have to be transparent and need to allow proper and transparent mechanisms for appeal. Governments also have to prioritise the access that victims and survivors of online abuse and gender-based violence have to justice. This does not only include improving law enforcement agencies' responses and awareness of the issue, but also demands an evaluation of entire judicial systems' ability to respond effectively to victims' and survivors' needs. Where possible, the creation of specialised and fast-track agencies and courts (including such online measures) to help victims and complaints with complaints should be explored.

155. The BPF also found that there is much uncertainty regarding intermediaries' responsibilities in addressing and countering online abuse and gender-related violence. There is a clear need for the public sector to evaluate its legal relationship with intermediaries in this regard, including the level of obligations it can realistically impose on intermediaries. Any duties imposed upon intermediaries, however, need to be both flexible to account for technological change, and workable to account for the nature and speed of content distribution.

156. While the responsibility of educating users and improving digital literacy levels arguably lies primarily with the public sector, BPF participants also suggested that the public sector should consider cooperating more closely with the private sector (particularly intermediaries) to ensure education also continues on relevant platforms.

157. Lastly, Internet intermediaries can explore clearer and more explicit commitments to comprehensive human rights standards to better address the issue of online abuse and gender-based violence. The UN "Ruggie Framework" can provide guidance on the actions they can take to ensure that women's rights online are promoted and respected in accordance with international human rights standards.

Iii. Other considerations

A better understanding of context and stakeholders

158. Whilst the importance of understanding different contexts has already been stressed, it is pertinent to highlight certain stakeholders and/or contexts that may deserve future attention. This includes the ways in which the issue affects girls. As mentioned in Part I, while most research on protecting children online are not gender-specific, some forms of online abuse and/or violence are more likely to affect girls than boys.

159. Some BPF participants highlighted the need to investigate the particular challenges that disabled women face online, but the BPF did not manage to find any research or examples of how online abuse and gender-related violence impact such communities. Further work needs to be done to investigate the challenges disabled women may face in this issue.

160. BPF participants repeatedly stressed the importance of the technical community's responses to online abuse and gender-related violence, the BPF found it difficult to gather examples of technical community responses to the issue. Future work should pay more attention to gathering these examples and to working more closely with technical communities in addressing the issue.

161. The BPF also encountered some concerns as to the scope of the group's work, including questions about why the work only focused on women. Whilst the

reason for this mandate and scope is explained in Part II of Draft F, future research could consider investigating the incidence of abuse and/or violence of men. In particular, research around protection of children's rights online can make a distinction between girls and boys.

162. Lastly, the various dimensions of abuse and violence in online contexts are also important to study, particularly where different perceptions of harm and the distinction between offline and online environments are kept in mind.

Thank you

The valuable input and contributions made, and hours of time invested, by various volunteer participants in different phases of this BPF's work are highly appreciated.

PART 2 - METHODOLOGY

A. MANDATE

i. The IGF and BPFs

1. The Internet Governance Forum (IGF), which was called for in section 72 of the *Tunis Agenda for the Information Society*,[119] brings people together from various stakeholder groups as equals in discussions on public policy issues relating to the Internet. While the IGF has no negotiated outcome, it informs and inspires those with policy-making power in both the public and private sectors. At the IGF's annual meeting delegates discuss, exchange information and share good practices with each other; aiming to facilitate a common understanding of how to maximise Internet opportunities and address risks and challenges that arise.

2. In 2011, the UN General Assembly (UNGA) Economic and Social Council (ECOSOC) Working Group on Improvements to the IGF published a report that called for the development of more tangible outputs to '*enhance the impact of the IGF on global Internet governance and policy*'.[120] To enrich the potential for IGF outputs, the IGF's Multistakeholder Advisory Group (MAG) developed an intersessional programme intended to complement other IGF activities, such as regional and national IGF initiatives, dynamic coalitions and best practice forums (BPFs). The outputs from this programme are designed to become robust resources, serve as inputs into other pertinent forums, and to evolve and grow over time.

3. BPFs, more specifically, offer substantive ways for the IGF to produce more tangible and substantial outcomes. While BPF outcome documents have already been useful in informing policy debates, they are also iterative materials that are not only flexible but 'living' in the sense that they can be updated at any time to accommodate the pace of technological change faced by Internet policymakers. BPFs have the freedom to define their own methodologies; tailored to each theme's specific needs and requirements. As decided in a general feedback session during IGF 2014, the term 'best' in BPF should be interpreted lightly because the topics of BPFs often relate to themes that need to be addressed in a flexible manner in order to accommodate the pace of technological change.

4. For 2015, the MAG identified six topics to form the focus of BPFs, including:

---

[119] World Summit on the Information Society (WSIS) (18 November 2005). *Tunis Agenda for the Information Society* (WSIS-05/TUNIS/DOC/6(Rev. 1)-E). Available online: http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html. [Accessed 28 October 2015].

[120] See page 4, UNGA ECOSOC (16 March 2012). *Report of the Working Group on Improvements to the Internet Governance Forum* (A/67/65-E/2012/48). Available online: http://unctad.org/meetings/en/SessionalDocuments/a67d65_en.pdf. [Accessed 28 October 2015].

- the regulation and mitigation of unwanted communications;
- establishing and supporting computer security incident response teams (CSIRTs);
- developing meaningful multistakeholder participation mechanisms;
- practices to counter the abuse of women online;
- creating an enabling environment for IPv6 adoption; and
- fostering enabling environments to establish successful IXPs.

ii. Defining the BPF's mandate

5. The MAG decided to devote one BPF to the study of practices to counter the online abuse of women. Facilitating dialogue and discussion on the issue of gender and Internet governance was seen as a critical issue by the MAG, and countering online abuse of women was seen as an increasingly important and focused area within this issue. Online abuse of women and gender-based violence constitute an acute manifestation of gender inequality and discrimination that seriously inhibit women's ability to enjoy fundamental rights and freedoms on a basis of equality with their male counterparts. There was also recognition that there are emerging and existing measures to address this issue, where the BPF is well placed to facilitate a multistakeholder discussion process in an attempt to collate research and good/best practices.

6. With BPFs having the freedom to define and delineate the parameters of their work independently, a consensus was reached amongst BPF participants at the early stages of its work that in order to truly address the problem, the topic should cover not only online abuse of women, but the range of actions and behaviour that constitute online abuse of women and girls and gender-based violence, of which abuse is a part of. Online abuse and gender-based violence also provides clearer policy frameworks to facilitate the discussion, building from existing efforts at the UN and other stakeholders working on the issue.

B. METHODOLOGY

i. Scope of work

7. The BPF provided an open and inclusive multistakeholder platform for the exchange of information on online conduct and behaviour that potentially constitute online abuse and gender-based violence, with the aim of collecting and compiling a helpful resource output for communities to create a safe and enabling environment for users online. The BPF's goal was not to negotiate text or to make concrete recommendations but rather to facilitate discussion and collect practices

that might help women to participate fully in the development of an inclusive and people-centred information society.

8. The BPF therefore asked all stakeholders to help it address the following question:

> *What are effective practices and policies that address, mitigate and/or prevent the abuse of women and gender-based violence online?*

9. In addressing this question, the BPF mapped priorities for its work in a draft outline of its proposed scope, namely:

Introduction & problem definition – to:

- define the problem in as much detail, yet also as flexibly, as possible; and
- identify the underlying factors that contribute to and create an environment in which abuse of women and gender-based violence online is possible.

Solutions, responses and/or strategies to counter online abuse and gender-based violence – to:

- identify existing policy and other measures;
- highlight common practices that have proven to be effective; and
- investigate the intended and unintended consequences of policy interventions.

Conclusion(s) – to:

- share insights gained as a result of the BPF's experience – and lessons for future research; and
- highlight unresolved issues where further multistakeholder cooperation is needed and proposed steps for future multistakeholder dialogue and/or actions.

In the course of the BPF's work, the structure of the document has been adapted to respond to inputs received, while bearing in mind the main areas of study.

ii. Working approach

General process and methodology

10. A dedicated and open mailing list was created for the BPF by the IGF Secretariat in early March 2015, and details for joining the mailing list were published on the

IGF's website. Two MAG members volunteered to help coordinate the BPF, and the IGF Secretariat appointed a rapporteur to assist the BPF in coordinating, organizing and reporting on the BPF's work.

11. The BPF coordinators and rapporteur thereafter adopted a semi-structured methodology by organizing fortnightly virtual calls in order to introduce the topic to participants, to encourage broader participation, to define the scope of the BPF, and to investigate a proposed methodology.

12. Fortnightly meetings were scheduled using Doodle polls, and after each meeting summaries and/or recordings were distributed on the IGF's intersessional and BPF's mailing lists as well as being published on the BPF's dedicated platform on the IGF's website.[121] When necessary – for instance when mapping the BPF's scope of work, defining the BPF's synthesis document, and gathering input on Drafts I and II – the BPF made use of open, editable online platforms like Etherpad, Google Docs and the IGF's review platform, all of which are freely accessible by most Internet users. Draft JP was distributed on the BPF's mailing list and also published for comment on the BPF's platform on the IGF's website; with comments being received over email and at the BPF's session at IGF 2015 (see section viii below). To facilitate the involvement of participants from regions that do not allow access to Google and/or Etherpad, documents were also made available in original MS Word format on the mailing lists.

13. The IGF's website was frequently updated to elicit input on certain aspects of the BPF's work, and regular BPF status updates were sent to the intersessional and BPF mailing list with calls for input and/ or other relevant information. When necessary, the mailing list was also used to send follow-up emails to elicit responses and to stimulate debate on specific topics. Social media platforms like Twitter and Facebook were furthermore used to encourage responses to the survey, to gather more examples, and to provide input on particular aspects of the BPF's work.

Terms of reference: defining the synthesis document

14. Before defining the BPF's terms of reference and intended scope, participants undertook a comprehensive mapping exercise on an open and editable web platform (Etherpad) with the primary objective of framing the topics and elements the BPF intended to cover. Input regarding this framing exercise was invited and received both orally (during virtual meetings) and in writing (directly on the document and via the mailing list). After the first three meetings of the BPF,

[121] As a result of the incidents mentioned in Appendix 5, the meeting recordings were removed from the IGF's website and made available upon request to protect the privacy and safety of participants.

a consensus was reached by participants that the topic covered not just online abuse of women, but more comprehensively, a range of acts and behaviour that constitutes gender-related online violence against women and girls, of which abuse is a part of.

15. These topics were extracted from the framing document and used as the foundation for a detailed non-paper which provided a coherent overview of the BPF's objectives, scope of work, methodology, and how participants can get involved in the BPF's work. As with other phases during the BPF's work, an open, inclusive, transparent and iterative process was followed to create the synthesis document.

iii. Populating outline of work

16. A skeleton outline of work was extracted from the synthesis document and subsequently populated from data gathered on the mailing lists, during the mapping exercise, and from other documents shared with the BPF group to form Draft 1. The skeletal Draft 1 was subsequently discussed and populated, section-by-section, during fortnightly virtual meetings. After each meeting the specific section being discussed was again shared with the mailing list and input was invited. Draft 1 remained open and editable on Google Docs for a number of months until mid-September, when Draft II was produced. Draft II therefore reflected a broad range of inputs and views to provide a foundation for detailed discussion on the BPF issue.

17. To augment the input from frequent participants, data was also gathered and incorporated into Draft II and subsequent drafts using two additional sources: a survey and both informal and formal case studies; all of which were also aimed at encouraging broader and more diverse stakeholder engagement in the work of the BPF. More details of these methods can be found in the section below.

iv. Encouraging stakeholder engagement

18. Due to the nature of the Internet as a distributed network of networks, addressing the online abuse of women and gender-based violence requires considerable input and cooperation from, and trust among, a multitude of stakeholders, including the technical community, private sector, civil society advocates and organizations, governments, international organizations, academic community, users, and young people.

19. In acknowledging and supporting the work that many stakeholders have already done and are doing to research, support and help counter online abuse and gender-based violence, including the positive contributions and achievements

already made, the BPF provided a neutral forum where a compendium of practices were gathered, with due recognition and attribution given to relevant stakeholders and participants for the work that has already been done in addressing the challenge of online abuse and gender-based violence.

20. For this reason the BPF prioritised the importance of engaging stakeholders from diverse fields in the BPF's work in order to have vibrant discussions informed by multiple perspectives. This includes, *inter alia*, inviting participation from individuals who have personally dealt with online abuse and gender-based violence, civil society groups that have done significant and extensive research in the area, intergovernmental organizations, and the private sector. A list of the identified stakeholders who participated in the BPF's work – whether through case studies, survey responses, attending meetings, commenting on draft reports, or participating on the mailing list by sharing information – is contained in Appendix 1.

v. Mailing list

21. In March 2015 a wide call was issued to the IGF mailing list to encourage participants to join BPF mailing lists, including this one. The coordinators also directly contacted individuals from various stakeholder groups to encourage broader participation. Stakeholders were invited to participate in fortnightly virtual meetings, by commenting on and visiting an online platform hosted on the IGF's website, and by following discussions on the dedicated BPF mailing list.

vi. Survey

22. To gather more input on some of the substantial questions that the BPF aimed to address, a survey was designed and published on Google Forms (see Appendix 2 for the survey contents and analysis).

Survey design

23. Survey questions were derived from the synthesis document to address specific sections of the BPF's scope of work. The questions were drafted and refined in consultation with the BPF's community after consultation on the BPF mailing list and during a virtual meeting dedicated to a survey planning session.

24. The survey focused primarily on two aspects of the BPF's work: defining the problem of online abuse of women, and measuring the impact thereof on both communities and individuals. Because the target audience of the survey was not defined and invitations to complete the survey would be sent to both experts in the field and general Internet users, the survey provided relevant background,

context and descriptions where perceived necessary. To encourage more stakeholder participation, the survey was also kept relatively short, with a combination of close-ended and open-ended questions; the latter providing the opportunity for more lengthy, substantive responses.

25. Responses were elicited over a period of one month by calls on the mailing list, social media (including tweets from the IGF's Twitter account), and emailed invitations to various mailing lists (including mailing lists within the Internet governance, academic and broader community).

26. A total number of 56 responses were collected, with the largest proportion of responses submitted by respondents who identified themselves as part of the civil society stakeholder group (41%), and the smallest number from the technical community (4%). It should be noted, however, that the identified stakeholder groups were not necessarily mutually exclusive. Of these stakeholders, 31 respondents identified their organizations, which varied from civil society organizations to police and government departments, universities, intergovernmental organizations, etc.

27. The survey attracted responses from a rich diversity of regions, particularly from developing countries. Of the respondents that identified their countries (52 out of 56 respondents), 25% were from Africa, 23% from Europe, 17% from Asia, 13% from Central and South America, 12% from the Middle East and 10% from North America. Within these regions a vast number of countries were represented. From the Africa region, for instance, survey responses were received from South Africa, Zambia, Nigeria, Ghana, Tunisia, Kenya, Cameroon and Uganda. There were a limited number of countries represented in the Europe region, however, with responses only being received from the UK, Estonia, Switzerland and Germany.

Survey analysis

28. The survey analysis was conducted with the goal of gathering a non-representative snapshot of stakeholder perceptions and comments on the topic of online abuse of women and to consolidate and identify common concerns, issues and definitions for further study and for incorporation into the main outcome document where relevant.

29. Due to the number of substantive responses for open-ended questions, many interesting comments and/or quotations were also highlighted for inclusion in the main outcome document. These quotations were edited slightly for style consistency.

Survey results

30. The full survey analysis is contained in Appendix 2, and where relevant survey responses have been integrated directly into Part I of this report.

vii. Case studies

31. Using the mailing list and online platform, stakeholders were further encouraged to submit formal and informal case studies or examples relevant to the work of the BPF. The coordinators and rapporteur also did a substantial amount of direct outreach to request input. Inputs were received from a diversity of individuals and countries, including Suriname, the Philippines, the Council of Europe, Afghanistan, Pakistan, India, Albania, the United Kingdom, Brazil, Estonia, Bosnia and Herzegovina, Argentina and Nepal.

32. The case studies are contained in Appendix 3, and where relevant lessons, examples and other content extracted and summarised from case studies were incorporated directly into Part I of this report.

viii. BPF participation at IGF 2015

33. During IGF 2015 in João Pessoa, Brazil, each BPF had a 90-minute session at its disposal to further its work. The BPF thus held an interactive panel to discuss not only the BPF's draft findings and recommendations for further exploration, but also the ways in which the problem of online abuse and gender-based violence can continue to be addressed at both the IGF as a critical platform for multistakeholder engagement on key internet policy, governance and human rights issues, and in other policy discussion spaces.[122]

34. With the aim of engaging a variety of stakeholders on different aspects/ themes of the BPF's work, the BPF contacted and invited stakeholders from the academic community, civil society, technical community, international organizations, multistakeholder organizations, private sector, and governments.

Panelists included:

Agustina Callegari (Personal Data Protection Center, Ombudsman's Office of Buenos Aires City, Argentina)
David Kaye (UN Special Rapporteur on Freedom of Expression)
Frane Mareovic (Director Office of the OSCE Representative on Freedom of the Media)
Gary Fowlie (Head ITU Liaison Office to the UN in New York, USA)

[122] The session's video is available online in English: YouTube, IGF, *IGF 2015 WK6 BPF Practices to countering abuse against women online* (11 November 2015). Available online: https://www.youtube.com/watch?v=6Ef_HSKW-n4. [Last accessed 27 November 2015].

Hibah Hussein (Public Policy Analyst, Google, USA)
Mariana Valente (Director: InternetLab, Brazil)
Narelle Clark (Australian Communications Consumer Action Network; Immediate Past President of ISOC (Australian Chapter), Australia)
Nighat Dad (Digital Rights Foundation, Pakistan)
Patrick Penninckx (Council of Europe Head of the Information Society Department, Bosnia and Herzegovina)
Rebecca McKinnon (Global Voices Online, USA)

35. The BPF's session took place in the format of a "talk-show", preceded by a thorough discussion of the BPF's methodology. Audience members and online participants were also invited to ask questions and provide input. A few comments made by participants during the session (including panelists and audience members) were incorporated into Part 1.

36. In addition to the BPF's dedicated session, the BPF also gave feedback on its findings in the context of the IGF intersessional theme *Policy Options for Connecting the Next Billion* during a main session event on 11 November 2015. The BPF spoke about its work in general and with particular relevance to the challenge of access.[123]

ix. Other methods

37. To raise more awareness of the importance of the issue, and to gather additional responses in respect of one section of the BPF's proposed scope of work, namely the consequences of online abuse of women, a social media campaign was planned for mid-October. A case study containing more details about the campaign and its consequences, including an attempted counter-campaign, are contained in Appendix 5.

38. As mentioned in paragraph 20 above, community input and comment was elicited on every draft of the BPF's work. For Draft I, for instance, an open and editable Google doc was used, whilst for Draft II the IGF's review platform was used. In respect of the latter, 96 comments were received. All of these comments were analysed using a thematic analysis approach and were, as far as possible, used to improve and update the report. All of the comments and related analysis are contained in Appendix 4.

[123] The session's video is available online in various UN languages: YouTube, *IGF 2015 Day 2 – Plenary – IGF Intersessional Work: Policy Options* (11 November 2015). English version available online: https://www.youtube.com/watch?v=7FuU7ZL6oUo. [Last accessed 27 November 2015].

PART 3 - APPENDICES

APPENDIX 1: CONTRIBUTORS

As mentioned in Part 2, one of the BPF's primary objectives was to encourage the engagement of stakeholders from a variety of stakeholder groups. The lists of participants below include participants during virtual meetings, participants in the discussions held on the BPF's dedicated mailing list, panelists at the BPF's session at IGF 2015 (audience members are not cited), contributors who submitted comments and proposed changes to various drafts – irrespective of the nature or extent of the contribution made – survey contributors and review platform commentators.

Note that some contributors preferred to remain anonymous, and others used pseudonyms. Due to the large number of people who participate at different times of the BPF's work, the lists remain subject to change and may be updated as and when reasonably required.

Lead coordinator: Jac SM Kee
Rapporteur: Anri van der Spuy

General contributors

Abhilash Nair
Agustina Callegari
Aida Mahmutović
Ana Kakalashvili
Angelic del Castilho
Anja Kovacs
Anna Polomska
Arzak Khan
Caroline Tagny
Clare Laxton
Constance Bommelaer
Courtney Radsch
Despoina Sareidaki
Ellen Blackler
Ephraim Percy Kenyanito
Erika Smith
Evelyn Namara
Fiona Vera Gray
Florensia Goldman
Furhan Hussain
Gary Hunt

Gisela Perez de Acha
Hera Hussein
Ineke Buskens
Jake Barker
Jan Moolman
Jennifer Breslin
Katerina Fialova
Katharina Jens
Laura Higgins
Lianna Galstyan
Lisa Garcia
Louise Bennett
Michael Nelson
Nighat Dad
Nik Noone
Patricia Cartes
Peter Dengate Thrush
Ritu Strivastava
Ritika Gopal
Sadaf Baig (Khan)
Sara Baker
Sarah Parkes
Shannon Pritchard
Subi Chaturvedi (co-coordinator at the initial stages of the BPF)
Suprita Sah
Susan Benesch
Zakir Syed
Zoya Rehman

Panelists at BPF's session at IGF 2015

Agustina Callegari**,** Personal Data Protection Center, Ombudsman's Office of Buenos Aires City, Argentina
David Kaye, UN Special Rapporteur on Freedom of Expression
Frane Mareovic**,** Director Office of the OSCE Representative on Freedom of the Media
Gary Fowlie, Head ITU Liaison Office to the UN in New York, USA
Hibah Hussein, Public Policy Analyst, Google, USA
Mariana Valente, Director: InternetLab, Brazil
Narelle Clark, Australian Communications Consumer Action Network; Immediate Past President of ISOC (Australian Chapter), Australia
Nighat Dad, Digital Rights Foundation, Pakistan
Patrick Penninckx, Council of Europe Head of the Information Society Department
Rebecca McKinnon, Global Voices Online, USA

Survey contributors[124] (57)

Name	Country	Organization
Michael Ilishebo	Zambia	Zambia Police Service
Gbadamosi John	Nigeria	Media Rights Agenda
Shiva Bissessar	Trinidad & Tobago	Pinaka Technology Solutions
Zied FAKHFAKH	Tunisia	Dot TN
Said Zazai	Afghanistan	National IT Professionals Association of Afghanistan (NITPAA)
Rapudo Hawi	Kenya	Usalama Forum
Zakir Syed	Pakistan	*
Shreedeep Rayamjhi	Nepal	Rayznews.com
Soraya Chemaly	United States	Safety and Free Speech Coalition and The Women's Media Center Speech Project
Bruno Zilli	Brazil	Latin American Center on Sexuality and Human Rights - CLAM
Olga TSAFACK	Cameroon	Individual Freelance Digital security Trainer and Human Rights activist
R Daniel	SVG	Danielcharles consulting
Heidi J. Figueroa Sarriera	Puerto Rico	University of Puerto Rico
Sally Spear	England	*
Jake Barker	United Kingdom	United Nations Association - UK
Dora Boamah	Ghana	Media Foundation for West Africa
Naomi Mercer	US	US Army
Ingrid Srinath	India	Hivos
Agathos	Brazil	*
Francis Ssekitto	Uganda	College of Computing and Information Sciences, Makerere University
Nadira	Palestine	ISOC
Jaya	India	Ummeed
Anna	USA	*
Arzak Khan	Pakistan	Internet Policy Observatory Pakistan
Angoda Emmanuel	Uganda	Lira Town College
Scherry Siganporia	India	GIZ India (German Development Cooperation)
Mayengo Tom Kizito	Uganda	Anonymous
Angelic del Castilho	Suriname	*
Catherine Nyambura	Kenya	Dandelion Kenya
Sarah	Uganda	SAFAUO

[124] This list contains only those survey participants who identified themselves and their countries.

Christina Lopez	Philippines	Foundation for Media Alternatives
Asabe Sadiya Mohammed	Nigeria	Bauchi State University Gadau
Florence Y. Manikan	Philippines	Department of Social Welfare and Development
Hazviperi Makoni	United Kingdom	Girl Child Network Worldwide
Marion Böker	GERMANY	IAW, WILPF, other
Clare Laxton	UK	Women's Aid

Commentators on review platform: Draft II *[Names are reflected verbatim]*

Ana Kakalashvili
Russel
D
George Orwell
Thoth
They
Ty2010
Johnnynumeric
Mohit Saraswat
Bryanna Hatfield
Anon13
Jay
Fran Mambles
Shreedeep Rayamajhi
David Lillie
Ashell Forde
J. Carl Henderson
Morgan Qualls
John Smith
Ian Bibby
Courtney Radsch
Lianna Galstyan
Conor Rynne
V.Z
Maria Paola Perez
Encel Sanchez
J
William C. Johnson
Ferreira
Agustina Callegari

Ellen Blackler
Lasershark
Erika Smith
Chester
Evelyn Namara
Theodore K.

APPENDIX 2: SURVEY

In this Appendix, Section 1 consists of the design, methodology and survey analysis, whilst Section 2 contains the original survey.

SECTION 1

DESIGN AND METHODOLOGY

Survey questions were derived from the skeleton document to address specific sections of the BPF's scope of work. The questions were drafted and refined in consultation with the BPF's community (henceforth 'the survey designers') after consultation on the BPF mailing list and during a virtual meeting dedicated to a survey planning session.

The survey (see Section 2 of this Appendix for the survey questions) focused primarily on two aspects of the BPF's work: defining the problem of online violence and/or abuse, and measuring the impact thereof on both communities and individuals. Because the target audience of the survey was not defined and invitations to complete the survey would be sent to both experts in the field and general Internet users, the survey provided relevant background, context and descriptions where perceived necessary. To encourage more stakeholder participation, the survey was also kept relatively short, with a combination of close-ended categorical and open-ended questions; the latter providing the opportunity for lengthy, substantive responses.

Responses were elicited over a period of one month by calls on the mailing list, social media (including tweets from the IGF's Twitter account), and emailed invitations to various mailing lists (including mailing lists within the Internet governance, academic and broader community).

Diversity of respondents

A total number of 56 responses were collected, with the largest proportion of responses submitted by respondents who identified themselves as part of the civil society stakeholder group (41%), and the smallest number from the technical community (4%). It should be noted, however, that the identified stakeholder groups were not necessarily mutually exclusive. Of these stakeholders, 31 respondents also identified their organizations, which varied from civil society organizations to police and government departments, universities, intergovernmental organizations, etc.

The survey attracted responses from a rich diversity of regions, particularly from developing countries. Of the respondents that identified their countries (52 out of 56 respondents), 25% were from Africa, 23% from Europe, 17% from Asia, 13% from Central and South America, 12% from the Middle East and 10% from North America. Within these regions a vast number of countries were represented. From the Africa region, for instance, survey responses were received from South Africa, Zambia, Nigeria, Ghana, Tunisia, Kenya, Cameroon and Uganda. There were a limited number of countries represented in the Europe region, however, with responses only being received from the UK, Estonia, Switzerland and Germany.

ANALYSIS

The survey analysis was conducted with the goal of gathering stakeholder perceptions and comments on the BPF's topic. The analysis was done to consolidate and identify common concerns, issues and definitions for further study and for incorporation into the main outcome document where relevant.

Due to the number of substantive responses for open-ended questions, many interesting comments and/or quotations were also highlighted for inclusion in the main outcome document.

Definition of online VAW

The first task of defining the BPF's scope of work was outlining what constitutes online abuse and online violence against women. The survey asked respondents to list examples of the types of behaviour that they consider to be within this ambit in their knowledge and/or experience. This was an open-ended question that received a total of 43 responses.

In the survey responses, proffered definitions of online violence against women and girls generally contained three common elements, including:

- range of action/ behaviour that constitutes online abuse and gender-based violence;
- impact to rights and harm experienced;
- the role of technology in enacting/ enabling online abuse and gender-based violence.

Many respondents also stressed the fact that online abuse and gender-based violence is also echoed in offline spaces, whilst some personal definitions also specifically recognised online violence/ abuse as a violation of women's rights.

Types of action/ behaviour

The list compiled below consolidates responses submitted during online virtual BPF meetings, through the mailing list and on the first draft outline document, published on a shared Google doc.

- Infringement of privacy:

  - accessing, using, manipulating and/or disseminating private data without consent (by hacking into your account, stealing your password, using your identity, using your computer to access your accounts while it is logged in, etc.)
  - taking, accessing, using, manipulating, and/or disseminating photographs and/or videos without consent (including revenge pornography)
  - sharing and/or disseminating private information and/or content, including (sexualised) images, audio clips and/or video clips, without knowledge or consent
  - doxxing (researching and broadcasting personally identifiable information about an individual without consent, sometimes with the intention of providing access to the woman in the 'real' world for harassment and/or other purposes)

- contacting and/or harassing a user's children to gain access to her

- Surveillance and monitoring:

  - monitoring, tracking and/or surveillance of online and offline activities
  - using spyware without a user's consent
  - using GPS or other geolocator software to track a woman's movements without consent
  - stalking

- Damaging reputation and/or credibility:

  - deleting, sending and/or manipulating emails and/or content without consent
  - creating and sharing false personal data (like online accounts, advertisements, or social media accounts) with the intention of damaging (a) user's reputation
  - manipulating and/or creating fake photographs and/or videos
  - identity theft (e.g. pretending to be the person who created an image and posting or sharing it publicly)
  - disseminating private (and/or culturally sensitive/ controversial) information for the purpose of damaging someone's reputation
  - making offensive, disparaging and/or false online comments and/or postings that are intended to tarnish a person's reputation (including libel/ defamation)

- Harassment (which may be accompanied by offline harassment):

  - "cyber bullying" and/or repeated harassment through unwanted messages, attention and/or contact
  - direct threats of violence, including threats of sexual and/or physical violence (e.g. threats like 'I am going to rape you')
  - abusive comments
  - inappropriate jokes that serve to demean women
  - verbal online abuse
  - unsolicited sending and/or receiving of sexually explicit materials
  - incitement to physical violence
  - hate speech, social media posts and/or mail; often targeted at gender and/or sexuality
  - online content that portray women as sexual objects
  - use of sexist and/or gendered comments or name-calling (e.g. use of terms like "bitch"/"slut")
  - use of indecent or violent images to demean women
  - exposing women to unwanted imagery that may impact them negatively
  - abusing and/or shaming a woman for expressing views that are not normative, for disagreeing with people (often men) and also for refusing sexual advances
  - mobbing, including the selection of a target for bullying/ mobbing by a group of people rather than an individual and as a practice specifically facilitated by technology

- Direct threats and/or violence:

- trafficking of women through the use of technology, including use of technology for victim selection and preparation (planned sexual assault and/or feminicide)
- sexualised blackmail and/or extortion
- theft of identity, money and/or property
- impersonation resulting in physical attack
- grooming

- Targeted attacks to communities:

  - hacking websites, social media and/or email accounts of organizations and communities
  - surveillance and monitoring of activities by members in the community
  - direct threats of violence to community members
  - mobbing, including the selection of a target for bullying/ mobbing by a group of people rather than an individual and as a practice specifically facilitated by technology
  - disclosure of anonymised information like address of shelters, etc.

- Limiting women's access and/or use of technology

  - limiting women's access to the Internet and/or online services that men are allowed to use

- Intellectual property

  - Stealing, manipulating and or abusing a women's intellectual property online, including ideas and/or content

Legislative/ research definitions submitted by survey respondents

'Violence against women' is defined in article 1 the Declaration on the Elimination of Violence against Women (United Nations General Assembly, 1993) to mean:

> *"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."*

Women's Aid report 'Virtual World: Real Fear' looked into online harassment, stalking and abuse and defined *online abuse* as:

> *"the use of the internet or other electronic means to direct abusive, unwanted and offensive behaviour at an individual or group of individuals."*

Research by APC on online VAW defines technology-related violence as encompassing:

> *"acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as phones, the internet, social media platforms, and email."*

The UN Broadband Commission for Digital Development Working Group on Broadband and Gender report on "Cyber violence against women and girls" defines cyber violence against women and girls to include:

> *"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."*

Online violence and its relationship to offline violence

Various respondents stressed that online violence not only permeates the offline sphere, but also often extends from offline environments (and patterns of abuse, like ongoing domestic abuse) into an online sphere (i.e. vice versa). Online abuse and gender-based violence thus needs to be studied whilst keeping the offline environments in mind.

Some relevant research shared by survey respondents in this regard:

Women's Aid research with nearly 700 survivors of domestic abuse who experienced online abuse from a partner or ex-partner found:

- For 85% of respondents the abuse they received online from a partner or ex-partner was part of a pattern of abuse they also experienced offline.
- Nearly a third of those respondents who had received direct threats stated that where threats had been made online by a partner or ex-partner they were carried out.
- Women's Aid believes that progress has been made over the past two years but there is still far to go to ensure that women are safe online

End Violence Research from APC was conducted in 7 countries as well as the mapping of online violence globally and in the aforementioned 7 countries.

Impact and consequences of online VAW

This section was designed using a combination of close and open-ended questions. Options were provided through existing research and work in this area by survey designers, with an open-ended option to ensure new knowledge could be captured.

Respondents were asked to tick what consequences they believed online VAW to have on individuals and communities respectively. A multi-option variable was provided: they could tick more than one, and an 'other' category was also provided.

Impact on individuals

The most common consequences of online VAW on individuals, according to survey respondents (see Table 1 below), are that women suffer fear, anxiety and depression (89% of respondents) and that they withdraw from online spaces and reduce the extent of their engagement with the Internet (83% of respondents). Other common consequences, according to survey respondents, include that women may consider or attempt suicide (66%); have their work and income affected (66%); and experience their mobility being limited and/or curtailed (64%).

It is notable that response rate for all options are relatively high (above 60%), which points to the significant and multi-dimensional impact that online VAW can have on women who experience them. Although the "Other" as an option was selected, no respondents listed the consequences.

Table 1: Potential impact on individuals	
suffer fear, anxiety and depression	88.7%
consider or attempt suicide	66%
withdraw from online spaces and engagement with the Internet	83%
lose their social networks and/or support	62.3%
have their work and income being affected	66%
experience their mobility being limited and/or curtailed	64.2%
Other	39.6%

Impact on communities

The most common effect of online VAW on communities, according to survey respondents (see Table 2 below), is the creation of a society where women do not feel safe online and/or offline (83% of respondents). Online VAWG also contributes to a culture of sexism and misogyny online (77%) and, in offline spaces, to existing gender inequality (74%). It also is seen to limit women's ability to benefit from the same opportunities online that men frequently benefit from (e.g. employment, self-promotion and/or self-expression) (69.8%). As a result, online VAW also contribute to the creation of a society where men and women cannot participate equally online (62.3%).

Table 2: Potential consequences for community	
create a society where women don't feel safe online and/or offline	83%
create a society where men and women do not participate equally online	62.3%
contribute to a culture of sexism and misogyny online	77.4%
disadvantage women, as they do not have the same opportunities for benefiting from the Internet as result (e.g. employment, self-promotion, self-expression)	69.8%
contribute to existing gender inequality in offline spaces	73.6%
Other	

In some of the other, open-ended survey questions, respondents also sometimes highlighted the impact and consequences of online VAW (e.g. in the question about defining online VAWG). These include (in no specific order):

- limiting and/or violating women's rights;
- physical or psychological damage, including public humiliation;
- making women feel unsafe;
- silencing individuals; and
- forcing women out of online spaces.

Enabling environments

The survey also aimed to identify underlying factors that can contribute to online VAW. These potential factors were identified and compiled by the survey designers from existing experience and research. A non-exhaustive list was provided in the survey and respondents were asked to tick all the relevant factors, and to cite any additional factors not identified (see Table 3 below). No respondents specified other factors, although 12% of the respondents did think there were 'other' factors involved.

The two most significant factors recognised as contributing to and/or enabling online VAW are a lack of awareness and recognition of online VAW (86% of respondents), and inequality and sexism offline that is reflected and amplified in online spaces (80%). This seems to point to an existing culture that accepts gender disparity and online VAW as part and parcel of interactions online, which renders it invisible and normalised.

The second highest group of factors selected were related to gaps in legal remedies and barriers to access justice. Namely, a lack of trained moderators, police officers, etc. available to respond to cases of online VAW (74%), and the lack of legal remedies available to respond to cases of online VAW (70%). This seems to indicate that greater regulatory guidelines are needed to, at a minimum, provide recognition of online VAW as a violation of rights. Second, it also points to the important role that first level responders play in creating a safer online environment that rejects VAW.

Women's unequal participation as decision makers in the development of technology platforms and policies was also recognised an important factor (68%), which may be linked to the lack of mechanisms available in online platforms to enable effective responses to cases of online VAW (66%).

Gender disparities in both access to the Internet and in terms of the skills of Internet users were seen as relatively less significant factors by the respondents (40% and 54%, respectively).

Table 3: Factors that might contribute to/ help enable online VAW	
gender disparity in terms of access to the Internet	40%
gender disparity in terms of skills in using the Internet	54%
inequality and sexism offline that is reflected and amplified in online spaces	80%
lack of awareness and recognition of online VAW as a serious issue	86%
women's unequal participation as decision makers in the development of technology platforms and policies	68%
inadequate mechanisms available in online platforms that enable effective response to cases of online VAW	66%
lack of legal remedies to respond to cases of online VAW	70%
lack of trained moderators, police officers, etc. to respond to cases of online VAW	74%
Other	12%

As with impact, in the other, open-ended survey questions, respondents sometimes also referred to factors that might enable online violence and abuse. These specifically included the ability to remain anonymous online and a sense of immunity that exists in the online sphere.

The responses provide an insight into measures that can be taken to address this issue. Although capacity building on skills is seen to play a role in creating a safer environment online, the responses point strongly to the need for addressing underlying structures of gender disparity and the culture of sexism that facilitates the perpetuation of online VAW. This includes the need for greater regulatory guidelines and measures to both provide recognition, as well as resources and prioritisation to train first level responders in this issue, and the need for more equal participation of women in technology development and decision-making.

Specific examples

Respondents also shared specific examples on particular cases of online VAW that were faced, which helps to outline the interrelated and complex dimensions of this issue. This can be read together with country case studies that provides more detailed illustration of how online VAW is experienced and responded to in different contexts (see Appendix 3). Note that these responses were not edited.

Respondent from Zimbabwe, residing in UK: I want my case and of about 109 women in Zimbabwe community in UK to serve as an example. All of us 109 women have suffered from one cyberbully. We are willing to be interviewed to help in the study because everyone is yearning to speak out about it. The results might help the world to understand violence against women. Our question is will the Human Rights Act be used to protect the online victims by Vio Mak in UK. Zimbabweans in UK are suffering… Online abuse is defined with my own personal experience. This is where one takes presents your information wrongly on their website with intention to put your reputation in disrepute. I live in UK where many other laws could have protected me but simply because this happens online police have said they can not do much yet the perpetrators are known. In her many fake websites a woman called Vio Mak who parades as a human rights defender has distorted the work I do for charity by misinforming the public. Daily she posts

defamatory statements about me or other women from Zimbabwe. She labels us fraudsters, prostitutes, witches and many cultural unacceptable names. This has caused me and other victims to be hated by the public. She has cyberbullied us almost daily. Two women almost committed suicide. Since she has assumed name Human Rights defender police in UK believes her and so she is untouchable. She threatens women with deportations as she claims she is linked to UK government. Employers who google victims have dismissed from work. She can pick on anyone from Zimbabwe and defame them. To me this is online abuse and violence against women done under guise of goof name.

Respondent from Uganda: Of recent in Uganda, there have been case of leaking nude photos of women and girls having sex (sextapes) by their enstranged lovers.

Respondent from Germany: Since a while I have seen a few threats by terrorists which have messages against all women or especially girls (The most brutal I saw: picture of a grown up 30 years old terrorist holding a 7-9 year old girl on a market place in public, posing for the picture, - I guess it was a yezidish girl- next to him saying that all those girls where being married as a loan for that kind of terrorists, that all those (girls) are their loan and slaves; I was shocked and twitter after my complaint deleted it;)Marion Böker, Germany: Since I use online media and options since long I remember having worked 15 years ago for a political party; I had to email a lot, had to be and wanted to be online; and felt harrassed by a group of men (they only write very long e-mails, or chat messages- in the night at 3 am or so; and they were calling me part of a feminist (communist, jewish...) conspiracy against men, they described them as victims of women like me and threatened me,- it was bad since the internet keeps that somewhat forever… I received threatening fascist emails which forsaw torture for me, and finalized with: we know you private address, we kill you- and the police to whom I reported categorized it only as a 'insult', may be because the e-mail started weith 'You cunt (bad word for vulva), but the police ignored all parts where they wrote about torture and my death. The report at the police ended in nothing: but impunity.

Other comments

The survey included a 'catch-all' question that asked respondents if they had any other comments regarding the definition, scope and/or issue of online abuse and VAW. The survey designers included this question with the aim of gathering any comments that other questions did not directly address and providing respondents with a space to share additional thoughts and advice for the work of the BPF. Where relevant, responses in this section have been incorporated in the analysis of other survey questions. For example, where a comment related to the definition of the issue, such comment was included in the survey question asking respondents to define the issue and analysed in that section.

- Lack of awareness/ need for literacy programmes:

  The awareness and visibility around this issue for younger people is still lacking. (Anonymous)

  I strongly think there should be a heightened awareness program about online safety and how to safeguard yourself. (Respondent from India)

- Youth:

Online Abuse/ VAW is best curbed in early stages through Child Online Protection. If children are taught on child online safety, they tend to grow up knowing the do's and don'ts in the online environment. (Respondent from Zambia)

- Proactive versus reactive responses?

  Online Abuse / VAW is a gradual behaviour that does not happen overnight but keeps growing if not stopped or controlled. Any form of intervention at any stage can help reduce the vices. (Respondent from Zambia)

  I am a Law Enforcement officer and I have seen how weak our laws are when it comes to combating Online Abuse / VAW. We have Re-active laws and not Pro-active ones. Until such a time we have Pro-active laws, Online Abuse / VAW will continue to disadvantage victims of the vices. (Respondent from Zambia)

- Importance of context

  Online VAW are inherited from offline social problems that we might have in our societies and these problems could vary from one community to another. In my mind, these studies could be customized at regional or local context, which will enable us to gather more accurate data about a community and what constitutes towards VAW so that appropriate and effective recommendations could be provided. (Respondent from Afghanistan)

- Importance of the technical community

  There should be a special team at National CERTs looking into Online VAW at a grass-root level so as to ensure elimination of VAW at the very basic level. Also, at the intergovernmental and global level (UN and other international organizations) the issue needs to be debated and a comprehensive framework built to fix this menace of VAW. (Respondent from Pakistan).

- Building awareness of female experts in the field

  I also think that men still, especially in infotechnology consider women as not equal - and awareness how good women really are in that field should be emphasized much more.

- Intermediary responsibility

  Internet intermediaries (ISPs, telephone companies, website hosts) also hide from the cloaks of their terms and conditions, they do not claim responsibility and have no accountability when online VAW take place using their platforms. (Respondent from the Philippines)

  Following work on the topic of online abuse and VAW social media companies such as Twitter and Facebook have improved their safety processes and organisations such as google highlight their policies on issues such as revenge porn more prominently. (Respondent from the UK)

SECTION 2
SURVEY CONTENT

The survey was conducted using Google Forms, which allows an unlimited number of questions and responses and user-friendly design mechanisms to aid the layout of the survey.[125] The survey contents are copied below (although the formatting is not reproduced).

SURVEY: Countering the Abuse of Women Online

This brief survey is the first in a series of two surveys designed with the aim to gather broader stakeholder input on topics that are of vital importance to the work of the Internet Governance Forum (IGF) best practice forum (BPF) on Countering the Abuse of Women Online.

All contributions will be used to guide our work, which is aimed at creating a compendium of practices that help to counter the abuse of women online.

Read more about this initiative here: http://www.intgovforum.org/cms/best-practice-forums/4-practices-to-countering-abuse-against-women-online

For questions, please contact the BPF rapporteur, Anri van der Spuy (avanderspuy@unog.ch).

* Required

Tell us about yourself

This BPF is an open and inclusive platform that aims to collect experiences from a variety of stakeholders. To get an idea of how diverse contributions are, we appreciate your responses to these two basic questions.

What stakeholder group do you belong to? *
Select closest option.

- ○ Government
- ○ Technical community
- ○ Civil society
- ○ Private sector
- ○ Intergovernmental organization
- ○ Individual user
- ○ Academia

[125] The survey as on Google Forms can be viewed here: https://docs.google.com/forms/d/1Az3fSQRX5nVlkMpReLz4Vtk8QWygHqqJRrSrbvK5ZS0/viewform?fbzx=3083091881606085133.

- ○ Youth

Where are you from? *
Please write only the country name where you are ordinarily resident.
What is your name?
You can remain anonymous if you choose to. If you don't mind telling us who you are, please write your name.
What organization do you work for?
You can remain anonymous if you choose to. If you don't mind telling us who you are affiliated to, please write your organization's name.

About online violence against women (VAW)

There is still a significant lack of awareness regarding what kinds of online conduct constitute abusive and violent behaviour. To address the increasing prevalence of online VAW in an effective manner, we need to understand how you perceive online VAW, the factors that enable and/or contribute to such conduct, and the impact that online VAW has on not only individuals, but also communities.

How would you define online abuse and VAW?
Please add specific references from research or other policy documents as you see relevant.

In your knowledge or experience, what are the types of behaviour of conduct that you think constitute online abuse or VAW?

What impact do you think online violence against women can have on individuals? Individuals suffering from online abuse and VAW may:
Choose most appropriate option(s). Please add any comments or thoughts as you see fit, or other effects that are not included in the list.

- ☐ suffer fear, anxiety and depression
- ☐ consider or attempt suicide
- ☐ withdraw from online spaces and engagement with the Internet
- ☐ lose their social networks and/or support
- ☐ have their work and income being affected
- ☐ experience their mobility being limited and/or curtailed
- ☐ Other:

What effect(s) do you think online VAW can have on communities? It can:
Choose most appropriate option(s). Please add any comments or thoughts as you see fit, or other effects that are not included in the list.

- ☐ create a society where women don't feel safe online and/or offline
- ☐ create a society where men and women do not participate equally online
- ☐ contribute to a culture of sexism and misogyny online
- ☐ disadvantage women, as they do not have the same opportunities for benefiting from the Internet as result (e.g. employment, self-promotion, self-expression)
- ☐ contribute to existing gender inequality in offline spaces
- ☐ Other:

What do you think are some of the factors that contribute to online VAW?
Please add to the list or elaborate on your thoughts in the 'other' box below.

- ☐ gender disparity in terms of access to the Internet
- ☐ gender disparity in terms of skills in using the Internet
- ☐ inequality and sexism offline that is reflected and amplified in online spaces
- ☐ lack of awareness and recognition of online VAW as a serious issue
- ☐ women's unequal participation as decision makers in the development of technology platforms and policies
- ☐ inadequate mechanisms available in online platforms that enable effective response to cases of online VAW
- ☐ lack of legal remedies to respond to cases of online VAW
- ☐ lack of trained moderators, police officers, etc. to respond to cases of online VAW
- ☐ Other:

Other advice & help
Do you know of any resources that could help this BPF's work?
Resources include research, reports, documents, etc. Please include a link to the relevant source, or otherwise cite the title of the publication, name of author(s), publication date and/or source.
Do you have any other comments or thoughts about the definition, scope and issue of online abuse and VAW?

Join us & make a difference

Are you interested in helping us address the challenge of online violence against women? We welcome all participants:

1. Join our mailing list for updates on meetings and other developments: http://mail.intgovforum.org/mailman/listinfo/bp_counteringabuse_intgovforum.org
2. Visit the BPF's platform on the IGF's website: http://www.intgovforum.org/cms/best-practice-forums/4-practices-to-countering-abuse-against-women-online#about
3. For more information, contact Anri van der Spuy (avanderspuy@unog.ch).

Thank you

We appreciate the time you spent in completing this survey, look forward to learning from your valued responses, and hopefully to welcoming you to our BPF in the future.

APPENDIX 3: CASE STUDIES

Overview

To encourage broader stakeholder involvement and the BPF's ability to benefit from lessons learned in diverse regions and countries, a significant amount of outreach was done to individuals and organizations in order to gather examples of online abuse in diverse contexts, to learn more about the measures taken to address such violations of human rights online, and to ascertain if any lessons could be learned about policy approaches that are effective in protecting women's rights online.

In this Appendix, the formal and informal case studies received are included without editing (besides changing font type and size). Where possible, examples from case studies below were incorporated directly into the results section (Part I of Draft F).

Summary of case studies received and relevant page in Appendix

NAME (organization)	**COUNTRY/ region**	**Page of Appendix**
Laura Higgins (Online Safety Operations Manager at SWGfL)	UK	89
Fotjon Costa (Head of ICT at Ministry of Energy and Industry, Albania)	Albania	91
Piret Urb (Ministry of Foreign Affairs, Estonia)	Estonia	96
Angelic del Castilho (Ambassador, MAG member, Chair of Foundation Kinkajoe)	Suriname	98
Bridget O'Loughlin (Head of Division, Violence Against Women Division, Council of Europe)	Council of Europe	102
Lisa Garcia (Programme Coordinator for Gender and ICT, Foundation for Media Alternatives)	Philippines	105

Said Zazai (president, National information technology professionals association of Afghanistan (NITPAA)	Afghanistan	113
Shreedeep Rayamajhi (writer, activist, blogger)	Nepal	114
Aida Mahmutovic (Internet Rights and Women's Rights Program, One World Platform)	Bosnia and Herzegovina	117
Dr Fiona Vera Gray (End Violence Against Women Coalition)	UK	120

LAURA HIGGINS
Affiliation: SWGfL – lead partner of UK Safer Internet Centre
Country: UK

Countering Online Abuse and Harassment of Women and Girls – A UK perspective

I work for SWGfL, the lead partner of the UK Safer Internet Centre (part funded by European Commission and UK Government Equalities Office) where I manage two online safety helplines.

Launched in 2011, the Professionals Online Safety Helpline is a service for the children's workforce, responding to issues affecting children such as online bullying or sexting, as well as issues affecting the staff, reputation or harassment for example. Since inception, the helpline has seen an increase in cases of sextortion of young people or staff, as well as online sexual harassment and what is now termed revenge porn. Teachers, Police Officers and Social Workers have been victims as well as young people. Whilst we were able to manage these problems via our existing service, we realised this was a much wider, and potentially hidden issue and began awareness raising via media and lobbying Government for support for victims who were not from the children's workforce.

We were delighted to be given funding for a 12 month pilot project to support all adult victims of revenge porn, which launched in February 2015. This project is to support victims and assist in the removal of harmful content, but also to provide some numeric evidence of the issue.
In addition to responding to calls from victims, the RP Helpline proactively reports and requests removal of content we believe to be abusive. We understand that some victims may wish to be notified that we find content so they can pursue legal action against their abuser. Where we find content that is easily linked to an individual's Facebook account we send a private message reaching out to victims and offering our support. While we appreciate this may be upsetting in the first instance, we believe that victims need to have control over their situation. This proactive reporting has two benefits - we are starting to get a feel for actual scale of content posted online without consent, and it is disruptive to the sites hosting it! There are still many sites which deliberately host RP, and it is those who we target to remove content and hopefully make the internet a hostile environment for abusive content.
Our relationship with internet companies such as Google, Yahoo, Microsoft, Twitter, Facebook, snapchat and Tumblr has been developed over several years and is multi-faceted, they keep us abreast of safety and reporting updates so that we always provide accurate advice, we provide advisory support to them such as beta testing new products or services, or providing feedback on language, child protection etc, and they also provide us with named contacts should be need mediate in a case due to its complexity. I believe these organisations do take user safety very seriously and we are delighted with the work done by them to minimise this content and assist victims. Likewise many adult content websites are proactive in removing images which breach user privacy.

There are currently multiple academic research projects in the UK focusing on either RP specifically, or generally the abusive of women online, I expect much of this research will be available later in 2015. The helpline has contributed to several of these studies, providing both quantitative and qualitative input. The helpline will be undertaking an external evaluation of the pilot phase and will make this available to the public in quarter two, 2016…

Case Studies

An unknown man found a mobile phone, and when a female started messaging (the girlfriend of the phone owner) he impersonated the owner and convinced the woman to send him naked images via the mobile. Once he had the images he set up a Twitter account and publically shared them.

A Muslim woman left her forced marriage; her ex who is not based in the UK is now setting up fake profile profiles saying she is a prostitute and offering her services and giving out personal details such as address and phone number. She has been disowned by her family and has men knocking on her door saying they have seen her Facebook page. Police are involved but as the perpetrator is outside the UK they have offered little support.

A Chinese female called to say her Manager at the restaurant she worked at filmed her in the shower and used this content to blackmail her into working for free. She escaped and started working at a new establishment, where her Manager later sent the video and accused her of various things such as theft. When we advised her to go to the Police she refused as her visa had expired and she was working illegally.

Fotjon Costo
Affiliation: Ministry of Energy and Industry, Albania
Country: Albania

General overview on violence against women and girls (VAW) and online VAW in Albania

Albania's Constitution proclaims equality between men and women, but in practice often women do not enjoy the same rights to their as men. This inequality is palpable in many areas of life.
Until the 90s, Albania wasn't committed to the international instruments or European level, to the fundamental rights sanctioned to them, systematically violated. The first attempts to study on domestic violence in Albanian became only in the mid-1990s, while individual efforts institutional study and explore on domestic violence are added. Despite the lack of experience of research in this field, these efforts are met and faced a number of difficulties that have dealing with the complex nature of the phenomenon of domestic violence.
Despite the work on awareness, especially over the past ten years to sensitize the public, have not socially changed.
The difficulty of studying the phenomenon increases even more if we considering that it takes place "behind closed doors" to the family. The only source information remains in most cases the victim, which in any case it is not free from prejudices and stereotypes that exist in its society or in the community where it belongs.
Violence against women is a complex problem that involves more than an act in itself in personal relationships between men and women. It is a social problem extensive rooted in attitudes historical against women and marital relationship. Victimization of women their spouses reinforced by the economic situation, mentality and traditions, little awareness of people about violence in families.
Violence against women has become and the more problems concern in society because many men feel threatened by the concept of freedom of women. The study of domestic violence difficult considering a number of myths that do not allow a deeper understanding of the problem.
Thus, in different communities and social environments divided opinions that "violence is only one layer or certain groups", "violence is a problems of the poor "," violated women have certain personalities who trigger violence against them ", etc.
Albanian customs and traditions inherited from the past a few forms discrimination against women in the family and in society, but not the type of torture, or other forms of maltreatment. The phenomenon of "blood feud" was revived after 90s, especially in some areas of the country, it has caused problems for women, but especially for children. Feud is a hindrance to a life their normal due to the difficulties that brings isolation of men and children. Cases when the feud was hit on his wife appear to rare. "Canun" is still practiced in Albania, particularly in the North. Unfortunately, after the 90s, there is a reactivation of this code.
Sexual violence is still considered a "disgrace" for women and some cases (especially in rural areas) entails forced marriage perpetrator "to put the honor of the country". However, in urban areas, the situation has changed, but in most rural areas of sub-urban wife it continues to be under pressure of the patriarchal mentality.
The first decade of transition, 1990-2000, was characterized the spread of the

phenomenon of trafficking in women and girls in order prostitution.

In January 2003 Albania's government presented the first report its standard implementation of the Convention "On the Elimination of All Forms of Discrimination against Women" (CEDAW), ratified by Albania in November 1993. The problems presented were as sensitive prostitution and trafficking in women and girls. Committee on the Elimination of Discrimination against Women, UN has provided many recommendations, activity which has led not only to the state mechanism, but the activities of all NGOs that support, assist and help violence of women and girls.

During the last years Albania is undergoing a period of deep and often dramatic social, political and economic change that is having a great impact on the life of Albanians as social, economic and political position. Gender equality is a principle that is new to Albanian society and has not yet been embraced by a significant percentage of the population.

Nowadays is changed more and more into equality and due to EU and International standards as Albania is EU member candidate and due to as a member of a lot National and International initiatives, strategies and conventions. However, Albania today is different as in social, political, economic, development, etc. due to deep and continues collaboration with Albania Governmental Institutions\Authorities, International\National\Local NGO's, civil society, private companies etc.

Albania today is member of a lot International and National : council's conventions, initiatives, strategies and agreements(as Council of Europe Convention on preventing and violence violence against women and domestic violence, National Strategy for Gender Equality and Gender Based Violence and the Family Violence 2011-2015 d on the framework of the joint program between the Albanian government and UN 2012-2016"), initiatives that required procedures for opportunities for collaboration with NGOs to provide relevant services for victims of this most acceptable, the method of monitoring and other methods, etc.

As this BPF address on the challenge of online VAW issues, I think that Albania is a very good opportunity to create this kind of initiative. As I mentioned above Albania the last 10 years has begun to be part of international convention and agreements to discrimination and violence against women and girls. So, until today Albanian government with collaboration with the international and national NGOs and other actors does not report any policy or other measures on online VAW as Albania is implementing the "National Strategy for Gender Equality and Gender Based Violence and the Family Violence 2011-2015 d on the framework of the joint program between the Albanian government and UN 2012-2016"). But this is not meaning that Albania is not facing the challenge of online VAW due to country's fast development in all fields.

I strongly believe that online VAW challenge it will be a great initiative for Albania as we current drafting the National Strategy for Gender Equality and Gender Based Violence and the

Family Violence 2016-2020 (in order to add it as an initiative and issue on this national Strategy) and also for BPF community.

In conclusion, through the BPF community consultation and the other discussion, proposes and guidelines on BPF session during IGF 2015 we would have the possibility to start this initiative in Albania that will an excellent opportunity for us to learn from your experiences and solution for our first steps starting from policy and other necessary measures (as necessary guidelines an organization issued, laws, convention and policies adopted on national and European level, tools and methods of reporting abuse on platforms, etc.) and continuously in the future.

Additional comments received on 17 September:

Below information are from some of the most important implemented steps-priorities and near future (within 2015-2017) priorities of Albanian Government on Gender Equality and Gender Based Violence and the Family Violence. So, the priorities that not started jet should be for sure part of "National Strategy for Gender Equality and Gender Based Violence and the Family Violence 2016-2020", as I have seen until now the online violence it's not proposed jet. But I will start to meet some colleagues from the government and charged Ministry and institution in order to advise and propose that we should include online violence program as an excellent initiative worldwide.
Also, I believe that my activation to the IGF regional and IGF 2015 event (if it will be possible to participate in Brazil) is an excellent opportunity for me to be introduced and to be closer with the experiences and the proposes from the experts, NGO's, International Institutions, courtiers that applying online violence and all of you that you are working in this initiative from the beginning.
Meeting, desiccations and advises from all the actors should be very important for me in order i can understand and propose which is the most important and possible applicable method in case of Albania and after that I can present it to the charged organization and governmental institutions.

***(Below some of the most important priorities that have been taken and the others that are on the way)**:*

Priorities for the future:

Has passed the time when gender equality was a goal for us is a condition without that we cannot speak of sustainable development and good governance, and this is achieved when we work for this condition to become the majority.
Improving coordination and expansion of social services for vulnerable categories / groups in need, especially victims of Domestic Violence. Priority remains single mothers. Strengthening the national gender equality mechanism. The priority is to establish and empower local gender employee network in all municipalities reorganized under the new territorial division.

Economic empowerment of women. Addressing and improving gender balances in employment, unemployment, women's unpaid work, training, qualifications and entrepreneurship.
Promoting and supporting gender budgeting initiatives at national and local level.
For reshaping the roles and responsibilities of women and men within the family through legal improvements (maternity paternity leave and flexible working hours mothers), education and public awareness. Education and awareness of men and boys away from traditional gender stereotypes.
Gender equality and the fight against gender-based violence and domestic violence remain our Government priorities for the period 2015-2017.
some more recent positive developments in this area:

1- National Gender Equality Mechanism.

National Gender Equality Council is actively involved in fulfilling its duties under the mandate, which were reviewed and supported concrete measures to achieve gender equality, economic empowerment programs for women; promoting women's entrepreneurship; promoting women's development initiatives in rural areas; transmission of messages through awareness campaigns against violence against women.

Sector re-bounded Gender Equality within the Department of Social Inclusion and Gender Equality, with a view to playing a more active role in the management, coordination, implementation and monitoring of interventions to advance gender equality.

Positioning 18 gender officials at the ministry level and the completion of the job description of their specific tasks under the Law on Gender Equality in Society, it resulted in a better exchange and real-time information, as well as improving some programs and strategies from a gender perspective.

The challenge for the future is the establishment and strengthening of national gender employee network in all municipalities reorganized under the new territorial division.

In this context, and in support of the reform of Social Services, Ministry has suggested that the mechanism of gender equality continue to be at the municipal level, are appointed / reappointed clerk gender domestic or building special structures equality gender in their local units.
2- gender budgeting. Already within the Medium Term Budget Program, we have 11 budget programs of 8 ministries in which are integrated gender perspective. During this year, working on participatory budgeting at the local level in the municipalities of Cities of Albania (Tirana, Këlcyrë, Permet, Vlora, Saranda). This process aims consideration and fair distribution of financial resources based on the needs of women and men, girls and boys in society.
The process will be ongoing.
3 - Analysis and improvement of legislation. It has completed a review of Albanian legislation by experts with the support of UNDP, in accordance with CEDAW and the Istanbul Convention, which will soon appear in the table consultation with stakeholders, from where to

start a process of undertaking legal initiatives by the respective ministries (***including my ministry***).

4 - Women in decision making. In the direction of increasing the number of women in political decision making we have positive results significantly, where in the last election was confirmed 9 mayor of 3 who were in past elections, and we are waiting for nearly half the members of municipal councils are women and girls. This result came as the political will of the Prime Minister, but also the cooperation with the Alliance of Women MPs, international organizations and civil society.

5 - Project "GENDER EQUALITY FACILITY ". At the direction of the Albanian Government and the support of the Austrian Development Agency, UN Women has begun testing the project "Gender Equality facility - Support Structure of the Government of Albania for the Promotion of Gender Equality".

This project aims:

To support the Albanian government in the transposition of EU requirements for gender equality through the implementation of strategies, social, plans, policies, budgets, responsible and gender-sensitive, and the allocation of funds and setting priorities at national and local level, including strengthening the national machinery for gender equality and support decision-making and coordinating bodies, so that the mechanisms of government to be self-sustaining in their operation and supervision of the implementation of these requirements of the EU (the acquis) on Gender Equality.

Government and charged Ministry \Institutions will continue coordinating and monitoring role regarding the agenda of gender equality and the fight against domestic violence of the government.

Sensitization of public opinion is another objective of our work, which is carried out continuously by taking every day more and more the size of a widespread campaign and coordinated at central as well as local.

All plans and common priorities for the advancement of gender equality and the reduction of gender-based violence and domestic violence, require a serious cooperation with civil society and international partners, and builds mutual trust the actions and joint initiatives to achieve ***de facto*** gender equality in Albania.

Piret Urb
Affiliation: Ministry of Foreign Affairs, Estonia
Country: Estonia

Reply to the questionnaire on the approaches adopted in ESTONIA to address online VAW.

3 September, 2015

1. What policy and/or other measures exist in Estonia to address online VAW? ('Measures' can include the informal actions a community took, guidelines an organization issued, laws, conventions and policies adopted both on national level and in Europe as a whole, tools for reporting abuse on platforms, etc.)

Technological change, along with radical economic reforms, has been a crucial component of Estonian transition since the beginning of 90s. Specifically, 'internetisation' has become one of the central symbols of the rapidly changing society, leading to a widely held perception of Estonia as a leading e-state. Internet has become an important part of everyday life, particularly for the younger generations.

Some examples of measures applicable in Estonia to address possible online VAW:

- The Ministry of Justice is coordinating the implementation of the Strategy for Preventing Violence, which was approved by Estonian Government on 27 February 2015. The strategy encompasses violence between children, abuse of children, domestic violence (intimate partner violence), sexual violence and trafficking in human beings. Although online VAW is not a separate topic of this strategy, measures to prevent cyber-bullying, sexual offences online against children etc. have been planned.

- In July 2012, the Ministry of Justice initiated proceedings to amend sections 151 and 152 of the penal code, which would lead to a new legal norm regarding hate speech-related legislation in Estonia.

- In 2016 Estonia will criminalize stalking. At the moment it is possible to prosecute stalking only when individual behaviours that are elements of it amount to crimes prosecutable under other legislation: Penal Code includes a crime called "Unauthorised surveillance" (§ 137).

- Women who suffer under online VAW can contact Web Constables (Police and Border Guard Board police officers, see https://www.politsei.ee/en/nouanded/veebikonstaablid/) who give advice on the Internet. Web-constables started to work since 2011; they are police officers working in Internet. They respond to notifications and letters submitted by people via Internet and train children as well as adults at issues of Internet security. There are no age limits and

preferred is correspondence in Estonian, English or Russian. Letters are responded to at the first opportunity or at latest within three working days.

- Safer Internet Project established to raise awareness of children, parents and teachers of how to communicate safely on the Internet. The project activities have been focused on trainings and awareness-raising events for children, parents, teachers, social workers and the general public as well; giving advice from the Children's Helpline 116111 (www.lasteabi.ee) for children and parents on safe Internet use by telephone, MSN and other IM solutions; the web-based information hotline www.vihjeliin.ee, which allows Internet users to provide information about web environments which contain material about trafficking, sexual abuse, violation of children's rights, etc.

- It is possible to apply a restraining order in civil and criminal proceedings to protect violence victims, incl. victims of cyber abuse and harassment.

2. Do you know if these approaches have been effective in addressing incidents of online VAW? Please explain.

There is currently no data concerning effectiveness of the above-mentioned measures specifically on online VAW.

3. Do you know of any impediments that were or are being faced in adopting and/or implementing these approaches? Please explain.

No.

Angelic del Castilho
Affiliation: Foundation Kinkajoe
Country: Suriname

The case of Suriname

On the request and as part of the preparations for the IGF 2015 I have conducted a survey among girls and women in Suriname with the aim to:

1. Get an idea on the occurrence of online violence against women and girls
2. How women and girls define this
3. If and how they deal with it
4. What is available legally to deal with this?

For this survey [Editor's note: completed by 34 people in total] the attached form (in Dutch) was used and it was distributed online by a core group of girls. There was also an interview with the police unit responsible for dealing with violence against women as well as with the organization "Stop violence against women".

The interpretation of the results is as follows:

Age and Gender

All surveyed are female. The majority are in the age range of 22-30 years old, followed by 30-45 years old. Around 15% were either between the ages of 16-18 or older than 45 years of age.

Internet use

All of the surveyed use the internet. The majority is 24 hours online, due to the mobile internet. A small number of the surveyed are less than 1 hour a day online

Social media

The surveyed are all users of Facebook. Over 50% also makes use of Google, while 1/3 are also on Instagram. A small group makes use of LinkedIn, Twitter and YouTube. It can be noted that many are also on WhatsApp.

Abuse of pictures online

There is almost a fifty/fifty split on surveyed who have experienced abuse of their pictures online and those who have not.

Those who have suffered abuse of photos shared that the majority of them took action by demanding that the person who was guilty of the act, immediately remove the photos. From the remaining surveyed they had emotional reactions as in feeling angry, ashamed, and sad. In some cases this led to them not sharing it with anyone. Only a very small percentage made a complaint to the police

From those that answered that they had never experienced this kind of abuse, the majority said that even though they did not suffer this kind of abuse they knew of others who had.

Intimidation online

The majority of the respondents said they did not experience intimidation online. Around 40% said they had experienced intimidation online.

All respondents felt that in Suriname the issue of online violence against women and girls was not taken serious by the authorities and the community in general.
They mentioned that even though it is said that you can report violence against women, that is not possible in cases where this violence is anonymous. There is no awareness created towards the young on the issue of cyber bullying. Those who have experienced this kind of violence themselves say that they know from experience that you have nowhere to go, no legal assistance or options. Due to the lack of awareness and information from the authorities many do not even understand what it means and feel like there is nothing they can do about it, nothing they can do to stop it. There are still girls who believe that you can start a serious romantic relation through the internet. There is no updating of the technology for tracing perpetrators. There are no institutions (NGOS) that deal with this kind of violence against women. Still there are many who see this violence against women as funny and that the women themselves are to blame. People are not willing to speak about it in a serious way. The respondents believe that it happens much more frequent and that there is never a sign of punishment. There are no known police investigations on this issue. When talking about violence in Suriname people are inclined to only think about physical violence.

How they describe online violence against women

The definitions received vary from the use of the internet to verbally hurt women and girls, to inflict mental violence upon women and girls; a form of online communication with the aim of hurting others, provide the wrong idea about people.
Purposefully hurt women and girls through verbal violence online. Taking pictures of people without their permission with the purpose of posing them online.
The posting of people's pictures without their consent with negative, untrue stories linked to them. Online sexual provocation, manipulating of pictures with the aim of ruining the reputation of the person, or public shaming, intimidating, bullying of women and girls.
For some respondents it was difficult to describe since they believe that there are also women and girls who allow for them to be abused and allow misuse of their pictures. In short the majority felt it was every form of gossip, negative statement or intimidation directed towards a girl or woman with the intent of destructing the person. Many times there was referred to naked pictures and sex video made under duress.

The most important steps to take to deal with this issue

As most important were mentioned:

1. Create awareness about online violence against women and girls
2. Create possibilities, procedures for tracing anonymous culprits
3. Measure out harsher punishment by the law
4. Develop new technology for tracing perpetrators
5. Create awareness and train girls, women in the safe use of the internet
6. File complaints with the police
7. Publicize the cases (by the police) as well as the seriousness of dealing with it
8. Teach boys and men more respect towards women
9. Teach about the positive use of Social Media
10. Clear instructions from the Police and other justice authorities on how to deal and where to go with complaints about violence against women and girls
11. Prohibit gossip sites and sites that make a habit of allowing for violence against women and girls

12. Increase awareness on the dangers and how to protect against these dangers that can lead to online Violence against Women
13. Teach girls and women about the importance of self-respect
14. Thorough investigation by authorities, publicize this so that women and girls know and feel protected

Consequences of online violence against women and girls

It was very revealing that the majority of respondents felt that one of the consequences of online violence against women would be women/girls contemplating suicide or even acting on the thought of suicide. In most other cases the respondents felt that the women and girls would become depressive and may use the internet less or not at all.

The reasons for online violence against women and girls are blamed by the respondents on the lack of proper laws and regulations for dealing with this problem. Second to this is the minimal punishment given to perpetrators and the perceived lack of respect for women/girls in men and boys. The respondents believe that also women and girls are not very experienced at the safe use of internet. There is not enough awareness created and/or information provided to enable women and girls to use the internet in a safe way. A few respondents noted that there is in a few cases also a lack of self-respect in women/girls themselves.

Anonymous sites and slander

The respondents stated that they feel that websites/webpages that allow for anonymous posting of slanderous or intimidating or gossip about women and girls should be prohibited. This was the point of view of the majority. A significant amount of the respondents stated that since they believe that this kind of use of the internet is inappropriate they will not even visit these sites. Some stated that they will not post on those sites, but do sometimes visit to just read and a very small amount shared that they do not take these sites serious.

Anonymous sexual molestation online

The majority of the respondents stated that they had never been victim on online sexual molestation. Around 15% of them had been.

Those who did encounter online sexual molestation in majority ignored it until it stopped. A large percentage of the respondents stated that they did not know what to do and who to tell. Some tried to find out who the perpetrator was and some told their parents. None of them went to the police to file a complaint. Some became depressed, sad, and ashamed and prayed for it to stop. A very small number reported it to the site through which it was done to them.

Reaction from Institutions dealing with Violence against Women

From reactions it can be understood that for now these institutions mainly focus on domestic violence. Online violence against women is not dealt with it, especially not by filing complaints. The institutions their social workers do assist these victims by providing counseling with the aim of mentally dealing with the issues and protect themselves from further abuse.

The role of the police

The police have had to deal with complaint letters that they received through the Attorney General, requiring investigation of molestation, intimidation and the spreading of pictures and insults through the internet. Especially women and girls, and to a much lesser extent men, filed complaints with the police. The police took note of these complaints and when the perpetrator was known to the victim, he/she was questioned and depending on the seriousness of the case

prosecuted in accordance with the law; arrest, arraign etc. In the case of anonymous perpetrators a warrant was obtained from the Attorney General allowing the telecom providers to track down the guilty parties. The police recognizes that online violence against women and girls is a growing problem, but regretfully they do not possess all the necessary tools to adequately deal with this issue. The police force is in the process of constructing a new department to deal with cybercrime. However the financial cost for purchasing instruments as well as training of the officers is a challenge.

Status of instruments of law

Recently our Parliament approved a law dealing with stalking. This law seems to allow for more preventive action than before, however there is no explicit and in-depth dealing with online violence against women. The focus is still mainly on domestic violence. There is only once mention of IT use in stalking, where it is stated that no contact is allowed between the stalker and the victim, also not thrugh the use of phones , computers or SMS.

Bridget O'Loughlin
Affiliation: VAW Division, Council of Europe
Country/ region: Europe

VIOLENCE AGAINST WOMEN ONLINE

The Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (hereinafter "the Istanbul Convention")[126] can become an important tool for addressing various forms of violence against women and incitement to gender-based violence through new information and communication technologies. It also places particular emphasis on the role of the information technology sector and the media in preventing such violence.

What does the Istanbul Convention say?

The Istanbul Convention requires States Parties to take necessary legislative measures to criminalise different forms of violence, including, in its Articles 33 and 34, respectively, psychological violence and stalking[127]. The definition of stalking includes following the victim in the virtual world, engaging in unwanted communication through any available means of communication and spreading untruthful information online[128]. Psychological violence, as well as sexual harassment, which, according to Article 40 of the Istanbul Convention should also be subject to criminal or other legal sanction, can both clearly be carried out online.

Furthermore, as far as violence against women online is concerned, the media plays a significant role. As it has a great impact in shaping opinions and mentalities, it can contribute in preventing violence against women by shaping how society views women and men and how it understands gender-based violence. Media has an immense potential for social change. It is therefore important to recall Article 17 of the Istanbul Convention.

Recognising the important role of the media as well as the private sector, Article 17[129] requires states parties to tap into this potential by encouraging the private sector, in particular the information technology sector and the media, to take on the issue of violence against women and help shape, elaborate and implement internal and external policies in this field. The first paragraph of Article 17 contains two different obligations

[126] The Istanbul Convention was opened for signature in May 2011 and entered into force in August 2014.

[127] It should be noted here that Article 78 allows States to reserve the right provide for non-criminal sanctions, instead of criminal sanctions for these offences.

[128] Explanatory Report of the Istanbul Convention, para. 183. Available at http://conventions.coe.int/Treaty/EN/Reports/Html/210.htm

[129] Article 17 – Participation of the private sector and the media

1 Parties shall encourage the private sector, the information and communication technology sector and the media, with due respect for freedom of expression and their independence, to participate in the elaboration and implementation of policies and to set guidelines and self-regulatory standards to prevent violence against women and to enhance respect for their dignity.

2 Parties shall develop and promote, in co-operation with private sector actors, skills among children, parents and educators on how to deal with the information and communications environment that provides access to degrading content of a sexual or violent nature which might be harmful.

for states parties. First, it requires states parties to encourage the private sector, the ICT sector and the media to participate in the development and implementation of local, regional and national policies and efforts to prevent violence against women and domestic violence. Second, it obligates states parties to encourage these sectors to set guidelines and self-regulatory standards in order to strengthen the respect for women's and girls' dignity and in this way contribute to the prevention of gender-based violence. Private companies may be encouraged to establish protocols or guidelines for example on how to prevent violence in the workplace and support victims.

Paragraph 1 of Article 17 also explicitly points out that state parties have to respect the fundamental principles of freedom of expression and independence of the media. Although existing standards such as the 2013 Council of Ministers Recommendation on gender equality and media and the legal framework of some member states include provisions on gender equality and/or violence against women in the content of media[130] , Article 17 of the Istanbul Convention attributes the task of preventing and combating violence against women through the media to the media themselves. Media organisations can contribute to this by introducing self-regulatory mechanisms, internal codes of conduct/ethics and internal supervision to promote gender equality, combat gender stereotypes, avoid sexist advertising, language and content, and refrain from the use of degrading images of women associating violence and sex.[131]

The second paragraph of Article 17 requires states parties to co-operate with private sector actors to equip children, parents and educators with skills for dealing with the information and communications environments that provide access to degrading content of a sexual or violent nature. Although there is no doubt that the Internet is an innovative and global resource that serves the interests of many of its users, it is not always a safe, secure, open and enabling environment for everyone without discrimination. Many aspects of internet governance are still fairly unregulated, providing myriad opportunities for the free access to, production and dissemination of degrading messages about women or girls, hyper-sexualised images, and incitements to or normalisation of violence against women. Such messages and images propagated through the Internet can have a negative effect by socialising children into harmful stereotypes and the acceptance of violence against women. There is also growing evidence of misuse of new technology and social media to exploit and target vulnerable young people, including girls, in the form of bullying, stalking, harassment, and threatening behaviour. Therefore, raising public awareness on harmful material and practices in the information and communication environments, and education programmes for children, parents and educators on the safe use of the Internet are essential. The aim of such programmes would be to equip children,

[130] Point 1 of the Recommendation CM/Rec(2013)1 of the Committee of Ministers on gender equality and media: "Unless already in place, member States should adopt an appropriate legal framework intended to ensure that there is respect for the principle of human dignity and the prohibition of all discrimination on grounds of sex, as well as of incitement to hatred and to any form of gender-based violence within the media." Available at https://wcd.coe.int/ViewDoc.jsp?id=2087343

[131] See Encouraging the participation of the private sector and the media in violence against women and domestic violence prevention: Article 17 of the Istanbul Convention, A collection of papers on the Council of Europe Convention on preventing and combating violence against women and domestic violence. Equality Division, Directorate General of Democracy, Council of Europe (forthcoming), for further information on Article 17.

parents and educators with skills to protect children's safety while using new information technologies, mobile phones, tablets and social networking sites.[132]

As regards your question on the effectiveness of the Convention, it is too early to tell. 18 member state of the council of europe have ratified it and a further twenty have signed it. The monitoring mechanism is currently being put into place and the first evaluations are expected in 2016.

Are there any other international standards or initiatives on the matter?

Violence against women online is a topical issue at the UN level as well. Among others, the UN Human Rights Council Working Group on the issue of discrimination against women in law and in practice recently adopted a report (2013) that says*: "The Internet has become a site of diverse forms of violence against women, in the form of pornography, sexist games and breaches of privacy. For women who engage in public debate through the Internet, the risk of harassment is experienced online, for example, an anonymous negative campaign calling for the gang rape of a woman human rights defender, with racist abuse posted in her Wikipedia profile. Female ICT users have publicly protested about sexist attacks."*[133]

Violence against women online also is called as "Technology-Based Violence Against Women" among activists. There seems to be a very active USA based NGO, *Association for Progressive Communications* (APC), which published many reports (attached in the email) on the topic, including recent legislative trends. Their contributions were quoted in the UN CSW reports.

[132] ibid.

[133] Para 66. Available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/132/51/PDF/G1313251.pdf?OpenElement

LISA GARCIA
Affiliation: Foundation for Media Alternatives
Country: Philippines

Brief Country Situationer and Cases from the Philippines

Internet penetration in the Philippines is now over 40% of the population (roughly 40 million of the over 100 million population). The young are most active when it comes to online activities, and Facebook is the most popular social media in the country. More and more, online space is becoming the gathering space of people, where they meet, discuss, transact business, or do advocacies.

At the same time, the Internet is a risky space for some. Cases of harassment, abuse and crimes using ICTs have been reported. The Foundation for Media Alternatives (FMA), a partner of the Association for Progressive Communications (APC) in its FLOW project collects cases of technology-based violence against women. The cases are available in ph.takebackthetech.net.

In the reports compiled by FMA [Foundation for Media Alternatives – partner of SPC], majority are those that involve the uploading of images and videos without consent. However, there are no official documents that can say if this is the trend in the country.

Over the last two decades, several laws for the protection of women and children were passed in the Philippines. The Philippines has an anti-violence against women and children law (Republic Act 9262), the expanded anti-trafficking in persons act (RA 10364), the anti-sexual harassment act (RA 8353), anti-rape act (RA 7877), Responsible parenthood act (RA 10354), and the Magna Carta of Women (RA 9710), the country's localized version of CEDAW, among others. However, it was only recently that policies and laws relating to ICTs are being put in place. In 2009, the case of an actress whose intimate video with her boyfriend landed and became viral on the internet (See case of "Ruby" below) was one of the more visible cases that tested whether the Philippines was ready to respond to cases of violence against women committed online. It was also one of the more visible cases that exposed how people view sexuality in the country.

To curb and address the emerging incidences of online abuse hurled against women and children, laws such as the Anti Child Pornography Act[134] and the Anti-Photo and Video Voyeurism Act[135] have been passed. The latter is seen as a deterrent to criminals trading on non-consensual sex-related images. The former however, though well intentioned, includes

[134] RA 9775 punishes those responsible for the production, advertising and promotion, sale and distribution, purchase and access (even for personal use) of pornographic materials that involve children (Section 3).
[135] RA 9995 penalises the taking of photo or video of a person/s performing sexual acts or similar activities or capturing the image of the private area of the person/s without consent; and also the selling, copying, reproduction, broadcasting, sharing, showing or exhibition of such coverage or recording

provisions, which may erode Internet rights. Herein lies therefore the dilemma of content regulation of the Internet.

The Cybercrime Prevention Act (RA 10175) provides another example of the on-going debates in regulating cyberspace. It was passed in 2012 to address crimes committed against and by means of a computer system, amidst broad debates as to its scope and effect on human rights.[136] A watered-down version has been since declared constitutional by the Supreme Court, which simultaneously struck down several problematic provisions.

One particular provision problematic for women and gender advocates was retained. This refers to the "*cybersex*" provision. "Cybersex" was defined as "the wilful engagement, maintenance, control or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, *for favour or consideration*."[137]

Women's rights groups and advocates were almost unanimous in criticising the provision for its vagueness and overly broad scope. In a statement, they pointed out that *"the law fails to consider the transnational nature of sexual violence in cyberspace where site owners or operators and buyers are beyond the jurisdiction of the Philippines"* and as such may pose *"more harm to women who are usual victims of sexual violence in cyberspace.*"[138] Further, the statement says that the law *"focuses solely on criminalisation, unmindful of its possible effects and without clear understanding of the inherent nature and characteristics of ICTs relating to violence committed against women."*[139] Rather than recognise a person's agency to express sexuality online, sexual behaviour would be effectively criminalised. Also, they stated that the provision failed to address the underlying causes of VAW and failed to harness ICT's potential to promote women empowerment.

FMA believes that there is still the need to look at the existing laws and policies in the country and see how relevant and applicable they are to existing realities. It is also necessary to evaluate the existing environment and see if these are responsive to the needs of those who have experienced online violence. For instance, the length of time that cases are heard and decided upon should be looked into because in many instances, women who file cases withdraw them or become disinterested in pursuing the case if it takes years before a hearing, much less a decision is reached by court.

FMA is also reaching out to women's organisations, government, the youth sector, and students, among others, to raise awareness about the issue of technology-related violence against women. Currently, we are also talking to game developers and encourage them to develop games that are gender-responsive and those that do not tolerate violence. We are also

[136] The passage of the law met with opposition from different groups. Fifteen petitions were filed before the Supreme Court to declare the said law as unconstitutional.
[137] Section 4(1)(c) of Republic Act No. 10175
[138] In "Delete, Undo, Retrieve," Statement on the Cybercrime Prevention Act of 2012 which was signed by several women's rights groups and advocates
[139] Ibid

scheduling a hackathon/game jam (this October) to develop a game that will feature stories of women survivors of VAW, and their strategies to curb online VAW.

The Internet is still new in the Philippines and access to it and to other forms of technology is still developing. Even some prosecutors, lawyers and judges have yet to fully understand it and apply it to technology-related cases they handle.

Online security and safety are also necessary. This is not to say that women should not let themselves be photographed or filmed in compromising situation. It is important to support women's bodily and sexual autonomy. If taking intimate photos and videos for personal use, best practices should be developed around keeping such photos and videos secure.

Additionally, based on the cases that we have, we also recommend the following:

- Address the root cause of the problem, of VAW
- Review the country's development agenda vis-à-vis women, focusing not only on reactionary measures but also proactive and preventive ones, and contextualizing the experiences of women and the manner by which these experiences interconnect and intersect along a wider continuum of violence
- Strengthen women's networks and transforming the gender unequal ICT infrastructure for women, capacity bldg. and training on ICTs and the creation of relevant apps and digital content for women
- Address the continuum of violence that women face all over the world, including through structural changes

CASES

The cases below are examples of how women are experiencing online abuse and violation of their rights. Similar cases can be accessed at ph.takebackthetech.net

Infringement of privacy: Accessing private data without consent

In 2012, five female high school students from a Catholic school in Cebu City had their photos taken clad only in their undergarments. The photos were uploaded on her Facebook account by one of the girls, and this resulted in the students being banned by their school to join the graduation march.

Apparently, a computer teacher at the school where the girls were enrolled learned from other students in the school that there were such photos posted online. Using the school computers, her students logged into their respective FB accounts and showed the photos to the teacher, including other photos showing the girls smoking and drinking alcohol inside a bar. According to the teacher, there were times when access to the photos were confined to the FB friends of the girls, but at times they can be viewed by any FB user (i.e., it was public).

The teacher reported the matter to the school's Discipline-in-Charge, who then found the girls to have violated the deportment prescribed by the school (e.g., engaging in immoral, indecent,

obscene and lewd acts; smoking and drinking alcoholic beverages in public places; posing and uploading pictures on the Internet that entail ample body exposure; etc.)

The students involved were summoned to see the school principal and they were castigated for their behavior. Further, as penalty for their behavior, they were barred from joining the graduation exercises in March 2012.

The mother of one of the girls filed a petition in court to allow her daughter to join the commencement exercises, and the court issued a temporary restraining order allowing the students to attend the graduation ceremony. Despite the issuance, the school nevertheless barred the students from participating in the graduation ceremony.

Thereafter, the petitioners filed before the court for the issuance of a writ of habeas data claiming, among others, that accessing the photos of the girls was an intrusion of their privacy, and that these were obtained illegally. The petition was denied by the court and thus, it was brought to the Supreme Court. Basically ruling in favour of the school, the High Court essentially declared that nothing is ever private on Facebook, thus putting the burden of safeguarding one's privacy online with the users. The doctrine of "reasonable expectation of privacy" on Facebook now seems to be eroded.

See Supreme Court decision: Vivares and Suzara vs. St. Theresa's College, GR No. 202666

Defamation: (sexualised) images, audio clips or video clips taken or distributed without consent

"Ruby" (not her real name) is a model, actress, and brand endorser who lives in the Philippines. Like many celebrities, Ruby sought cosmetic treatments, and in 2007, a man named "Dr. Yu" treated her at a well-known cosmetic clinic. Not long after, Ruby and Yu became lovers. Like most secret loves, their affair was carried out in a hotel room. The relationship soon fizzled out, but in 2008, Ruby received a tip from a reporter: a sex video involving her and Yu would be released. Sure enough, in December 2008, three videos of Yu and Ruby depicting their time together at the hotel were published online. Subsequently, people began downloading the videos and selling them as DVDs. Ruby maintains that she was unaware she was being recorded, whereas Yu contends that she knew there was a camera, but he was not responsible for uploading the images.

The videos went viral, and each time the videos were reposted, Ruby felt she was being violated again and again. Moreover, having already been labelled a 'sexy actress', she faced acute harassment and verbal abuse online following the release of the videos. One commenter writes, 'I really don't pity Ruby because she did it on herself…She gave a signal to the whole world that she's not the type of woman whom you will respect.' In fact, because at the time of their affair Yu was in a relationship with the owner of the cosmetic clinic, many believed that it was the owner and Yu who were the real victims. Another commenter states, 'Don't you all think that she maliciously has done a great harm to her own gender…Ruby is such a slut!'

Following wide circulation of the video, Ruby was diagnosed with depression and began to undergo psychotherapy. She says, 'I felt like I lost something - perhaps my confidence. For one year, I did not talk to people. I felt like there was nothing for me to say.' Ruby felt deeply betrayed by Yu, who she had once trusted. During this time, Ruby began to lose modelling assignments and product endorsements as a result of the video scandal.

Alongside the 3 videos of Ruby that were released, other videos containing sexual content featuring Yu and other women were uploaded as well. Ruby was the only one who took the case forward; however, instead of being lauded for her bravery, she was seen as airing her dirty laundry in public, and received further abuse.

In May 2009, 6 months after the videos were made public, Ruby and her two lawyers filed a complaint with the National Bureau of Investigation, which recommended the case to the Department of Justice. Here, a criminal case against Yu was filed under the Anti-Violence against Women and Children Act, where Yu was charged with videotaping sexual intercourse and uploading the video without Ruby's consent. Simultaneously, Ruby filed a civil medical malpractice lawsuit against Yu, and a libel case against Yu's mother for slanderous statements she made in a TV interview. In December 2009, the criminal court dismissed Ruby's case on the grounds that Ruby was aware of being filmed, and that the uploading of the video could not be traced back to Yu. One possible reason for the dismissal was that there was no legal provision for ICT-based violence against women at the time, which weakened Ruby's case. Furthermore, the accused was not required to testify, which Ruby believed biased the courts against her. However, in November that year, following Yu's suspension by the Philippine Medical Association, the Professional Regulations Commission revoked Yu's medical licence, securing at least partial justice for Ruby.

In their attempts to discover who originally published the leaked video (it turned out that the clinic owner and others had access to Yu's hard drives), the NBI tracked down the first website that uploaded the video - fleshasiadaily.com, a porn site based in Cavite. The website owners claimed they received the videos from an unknown address; however, because intermediary liability law is unclear, they were not compelled to share the address with law enforcement.

The most crucial and empowering element in Ruby's fight for justice was the support she received, which included her then-estranged father, a friend who helped her with financial expenses, and perhaps most importantly, other people from the acting industry who publicly supported her. Another source of support for Ruby was a women's organisation, which provided her with counselling and allowed her to share her story with other women survivors of violence. The support and strength of other women who could relate to her story made Ruby realise that 'If [I did] not confront it now, it will hound [me] later.' Alongside her family, friends and colleagues, two provinces in the Philippines declared Yu as *persona non grata*, giving Ruby further confidence to pursue justice. Indicative of her strength, Ruby was quoted as saying, 'I intend to fight, win or lose. Whatever happens, at least I have fought for my rights.

At least people are realising that what was done to me was wrong…if you keep quiet for life, more women will be victimised.'

Ruby's courage to speak and fight was not in vain. Just before Ruby filed her case, a Senator delivered a speech on the issue, and later that year, the Senate conducted a related inquiry. One Congressman was quoted saying, 'If not for Ruby who fought for her right, people would not have noticed the importance of the law.' The law he was referring to was still awaiting approval by the Senate, but by early 2010, the Anti-Photo and Video Voyeurism Act was signed into law.

Case summary taken from
http://www.genderit.org/sites/default/upload/case_studies_phil2_1.pdf

Repeated harassment through unwanted messages & contact; Direct threats of violence, including sexual and physical violence; Doxxing (researching and broadcasting personally identifiable information about an individual without consent)

A woman who wrote to FMA said she was informed by her sibling that someone saw her photo wearing bikini in a certain website Reddit. At this time, she called up her former boyfriend (who had photos of her in his mobile phone; but according to the boyfriend his phone got stolen). Her reputation was slightly destroyed seeing as how her photos were published without her consent or approval. She emailed and reported to the website administrator the person responsible for uploading the link and shortly it was taken down. However, the online harassment was repeated. A friend contacted her informing the same scenario. With disappointment, she just decided to say that the photo was edited and not her.

The same woman said she also received an email from someone with abusive and threatening comments.

""I know what you want you slut" and also two photos of p****, when I asked "Who are you?" the reply was "Someone who would give you what you deserve" and then also sent one photo of me in a private nature and threatened that if I didn't reply, he would spread it in the internet. I did not reply after that."
She got paranoid that those photos would surface in the Internet. She decided to look for the source of these email. She made use of the available email trace headers and IP and reported it. However the IP address came from California, USA and she was not sure if the email really came from there or if the abuser made it so. After that, she found a site where she can search a name, email address, so the results would show a list of people. She then used the a certain cite to search for used email and was link to another site where she apparently found her Google+ account with the picture of her wearing a bikini. She was added to a person's circle and that person named "Rey Pinyoko" (pun for Rape Me) then proceeded to post more private photos of her with lewd captions and malicious comments.

The woman said she was emotionally disturbed and did not know who was really responsible

for this. She wanted her photos removed but she said she did not think that Google+ is acting on such abuses.

Damaging reputation, credibility; Infringement of privacy

On July 10, 2015, alleged videos of a 12-year old female young actress masturbating were posted and went viral online. According to reports, they were first uploaded in a Facebook fan page until they spread and went viral. Sources said that the videos of young actress were taken in different areas of their house. One was taken in the bedroom while the second video was taken inside the bathroom. There were those who claimed that the girl in the video just looks like the actress. However, there were photos allegedly proving that the bedroom in the video is the same bedroom shown in the photos of young actress' Instagram account. Netizens reacted and believed that it was not the young actress, but her older sister. Photos circulated in other social media accounts show that the two sisters really look-alike.

Majority of the netizens are still puzzled whether the alleged scandal is true or just made up by someone to destroy her reputation. To date, it is not known yet who uploaded the videos. There was also a report that the young actress' mobile phone was stolen two months before the videos went online.

There is still no statement from the young actress' side about the videos but her fans are continually giving their support and urging people to stop sharing and spreading the said videos.

Sources: http://www.manilalink.com/2015/07/star-andrea-brillantes-scandal-video.html; also http://www.tahonews.com/girl-on-andrea-brillantes-scandal-video-is-not-her-but-her-older-sister-photo/

Abusive comments; Verbal online abuse; Hate speech targeted on gender and sexuality; Mobbing

A female human rights advocate posted a photo of her on Facebook with the hashtag #OOTD (outfit of the day) and the question" Is my dress provoking you?" This is actually an experiment she was doing to document street harassment of women. She shared that she received catcalls and stares from men for wearing the dress. The same post received over two thousand shares and 115 comments. The comments showed a thread of discussion where some men were somehow "defensive" saying not all men treat women as sexual objects. She received criticisms for a thought provoking post and was called names. The one who posted the photo replied to all comments and even blogged about her experience. She also had other women sharing similar experiences.

"Ever since that post I made was shared over a thousand times, I have gotten several comments from men saying I am sexist, saying if I want to be respected I should always wear decent clothes, saying not all men, saying I am just a feminist who hates men, saying I judge people, saying I don't listen to their side, saying I don't empower women because I portray us as victims of society. They have tweeted me, messaged me, tagged me in posts..."

"One man told me I am trying to make every woman a victim, but aren't we all are? And is there shame in being a victim? Isn't one way to be empowered is to acknowledge that you are a victim and rise above it? Because we have to recognize that we are victims in order for us to understand what victimizes us and how to tackle it, which in this case is a sexist and patriarchal society."

See reneekarunungan.com

Sexualised blackmail or extortion

The National Bureau of Investigation arrested 13 suspects in a series of raids against alleged cybersex dens engaged in online sextortion. The NBI authorities explained that the suspects were engaged in sextortion. Men or women who patronise the services of the operator's cybersex website are unknowingly recorded. After which, they are threatened with online exposure unless they pay off the cybersex operators. The extortionists can ask for huge amounts, depending on the victim's profile. According to the report, the suspects also allegedly used minors to advertise their website.

It was not reported however, if those luring clients, mostly foreign clients, were coerced into the work that they are doing.

Source: http://www.gmanetwork.com/news/story/353315/news/metromanila/nbi-arrests-13-in-series-of-cybersex-den-raids
See also http://www.theguardian.com/world/2014/may/02/philippines-cybercrime-suspects-sextortion-swoop

Said Marjan Zazai
Affiliation: President of National information technology professionals association of Afghanistan (NITPAA)
Country: Afghanistan

Example from Afghanistan

Internet usage has grown over the years in Afghanistan. Some statistics say the overall internet penetration to be 5% which is around 1.5 million people. Literacy rate, mobile phone use and working individuals' ratio is higher among women which could indicate that there are more men using the internet than women but the number and impact in the society is pretty large regardless of the ratios. In a recent study performed by BBC (http://www.bbc.com/persian/afghanistan/2015/08/150823_k04_afg_women_problem_in_facebook?ocid=socialflow_facebook#share-tools) which is published in Persian titled as "From naked pictures to fake accounts: Headaches of Afghan women on Facebook", brings stories and real cases of Afghan women who face problems using social media on the internet. Majority of the examples are related to Facebook but it can be seen across other social media networks.

These stories are examples of what actually happens with women online in Afghanistan. Men usually send friend-requests or inappropriate text messages to women they don't know. They are harassed when they post comments or publish their pictures. Their pictures are stolen and fake accounts are created to defame them or destroy their reputation in the society. Naked pictures or other forms of sexual material are transmitted to them which forces women to use aliases and take down their pictures or they shut down their social media accounts.

Another contribution to this social dilemma is added by IT staff in professional working environments. As someone who has worked as an IT support staff for years and have come across individuals who violate their rights as IT support staff and get access to employees' computers without their knowledge, i acknowledge this being practiced across many organizations without the knowledge of the senior leadership. The one example that i can confirm is an organization in the capital where the chief IT officer installs remote access software on women employees' computers, collect their data and screenshots and then blackmail them. The psychological threat to their defamation or threat to share their data with their bosses leads to the fulfillment of the desires of the chief IT officer. The data being used in most cases is the email conversations or chat logs among other colleagues which could be about their boss or someone within the organization.

The lack of organizational policies and national laws governing privacy and security of individuals lead to the abundance of such cases in developing countries where such stories are not told or published because there is no benefit to the victims. These cases are repeated without the offenders being punished at the organizational level or taken to court.

Shreedeep Rajamayhi
Affiliation: Blogger and activist: http://womenoutcry.blogspot.com/
Country: Nepal

Online abuse of women and current practice in Nepal

Definition:

Online abuse or exploitation of Women or Violence against of Women is a condition where a woman is being threat in any way to think beyond her comfort zone. The unwanted situation can be described as a threat or unintentional comment or slang or any sort of behavior that triggers her to the uncomfortable zone both mentally or physically. The action is completely subjected to the intention of the provoker where the persistence of the action signifies the intentional action to be online abuse or exploitation.

Current types of online abuse or exploitation:

1. Email threats
2. Use of sexual slangs and words
3. Sharing pornographic images and videos
4. Sharing Unwanted links
5. Tagging people in social media Sites
6. Use of photos of woman without their consent
7. Sending irreverent Message in social media
8. Editing and compiling pictures
9. Promoting and circulating nudity
10. Adult jokes and picture
12. Blackmailing

Solution:

1. Awareness programs about online privacy and vulnerability
2. Privacy in optimization of social media tool
3. Clear core values of internet
4. Standardization in policy
5. Effective CISRT mechanism
6. Understating the importance of social media
7. Importance of setting device
8. Training for teachers

Nepal's Situation:

Nepal has been dealing with this cybercrime specially related to social media and fraud under the Electronic Transaction Act 2006. There is no specific law or section that defines the nature of online abuse or exploitation of Women or Violence against of Women.

There has been a definite rise in cybercrime cases in Nepal in absence of proper policies and

mechanism. There has been a rise in the report of such crimes, and police statistics show that they had increased by as much as 105 per cent in the last fiscal year, 2014-15. Figures show that a total of 39 cyber-crime related cases were reported to the police last year while such crimes numbered 19 before that year. Moreover, these cases are on the rise in the recent year with as many as 35 such cases reported to the police after mid-July in the beginning of this current fiscal year. The major cybercrimes that take place are, among others, E-mail theft, data hacks, online fraud and impersonating profiles.

Current Law Practice in Nepal

The Electronic Transactions Act, 2063 (2008)

Article 47

Publication of illegal materials in electronic form: (1) If any person publishes or displays any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to the public morality or decent behavior or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities shall be liable to the punishment with the fine not exceeding One Hundred Thousand Rupees or with the imprisonment not exceeding five years or with both. (2) If any person commit an offence referred to in Sub-section (1) time to time he/she shall be liable to the punishment for each time with one and one half percent of the punishment of the previous punishment.

Future Plans

In terms of cyber policy and proper mechanism to monitor the cybercrime, the Nepal Government recently has shown commitment towards establishing a National Cyber Security Strategy to deal with such threats and attacks. The government is committed to make cyberspace safe in Nepal and bring Child Online Protection (COP) and also a new law for cyber security.

Sample case of online women abuses

1. Youth arrested for sharing sex video

Link: http://womenoutcry.blogspot.com/2015/07/youth-arrested-for-leaking-sex-video-of.html

2.A man arrested for hacking and blacking woman sharing obscene picture

Link: http://www.rayznews.com/police-arrested-a-man-with-fake-facebook-account/

3. Report on online sexual exploitation of 2014

Link: http://www.rayznews.com/online-abuse-and-women-sexual-violence-in-rise-in-view-of-current-technology/

About the researchers

I am a writer, activist, and blogger. I believe in standardization & in the version of Internet for all. I am also a Diplo foundation Graduate of the **Internet Governance Capacity Building**

Programme 2009(IGCBP09) with security as my major & have published a research paper on cyber warfare & terrorism.

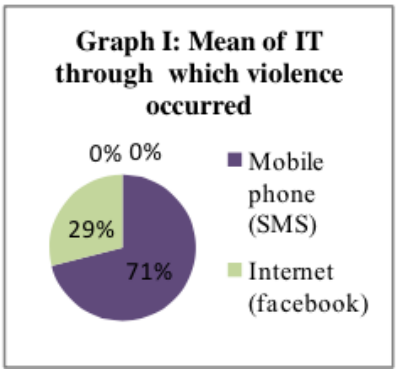
I have been regularly following and writing blogs and articles of Internet Governance Issues. Since last 10 years, I have been directly involved with various aspect of standardization issues and have been attending the IGF regularly. I have written and raised various articles and issues related to Human Rights, FOE, Privacy, security.

Aida Mahmutovic
Affiliation: One World Platform
Country: Bosnia and Herzegovina

PART 1

This report is the result of collaboration between One World Platform with Centre of Legal Assistance for Women in the city of Zenica, as a part of efforts for proving the real existence of tech-related VAW, and under APC's FLOW project "End violence: Women's rights and Security online", funded by Dutch Ministry of Foreign Affairs.
One World Platform is FLOW partner organisation in Bosnia and Herzegovina.

Data used in this research is based on processed information provided to One World Platform's research purposes by Centre of Legal Assistance for Women Zenica for year 2012.



During the following year Centre provided over 2000 legal services. From total number of legal services provided, 750 cases were in domain of Family law. Every fourth client experienced cyber bullying (202 clients). Violence, like other forms of harassment were done mostly by SMS (141 cases), 58 clients reported that they were harassed via Facebook.

Often after threats were made virtually via SMS and Facebook, abusers continued their harassment in person.

Interesting data is that clients from urban area were more exposed to harassment via internet, while clients from rural area weren't exposed to that kind of harassment except threats made via SMS. Harassment and stalking included sending multiple threats or false accusation via email or mobile phone and putting them at risk.

Looking at the level of education of clients (total number of 202), the highest number of clients exposed to this kind of harassment 162 of them had secondary education, 35 of them had university degree and only 2 of them had degree from primary school.

1. There weren't any major obstacles in excess to data because we had a database from which we were able to take all the needed data. However we didn't pay attention on how testimonials were conducted from clients which happened to them via internet and mobile phones. Orally, clients would explain their problem in detail and we would record that. However we didn't use it to make official written submission and to us that information wasn't as relevant as it should have been in using it to map violence. I have to state that every case from 2012 had to be examined to find elements that are focus of this research.
2. It was surprising for us that huge number of clients recognized this kind of violence and sought protection. Unfortunately, expert assistance wasn't provided to them on how to protect themselves when it comes to IT violence and abuse, and especially when it comes to identity theft and making false Facebook profiles. A case like that happened to one of the lawyers in our organization. After filing complaints to the police and prosecution, proper punishments weren't found even though evidence existed.
3. Steps that we made after initial research are modifications of record forms which are related to the clients, adding, filling in and entering data in database.
4. While providing legal aid to the clients, after the meeting with the staff of your organization and highlighting the problem we changed the course of our thinking and realized that we have data which we didn't use nor did we warn them about this problem even though a large number of evidence existed for this kind of violence.

Our vision is that in the next period we pay more attention to this problem and do legal analysis with reference to this problem.

PART 2

This report is the result of collaboration between One World Platform with Centre of Legal Assistance for Women in the city of Zenica, as a part of efforts for proving the real existence of tech-related VAW, and under APC's FLOW project "End violence: Women's rights and Security online", funded by Dutch Ministry of Foreign Affairs.
One World Platform is FLOW partner organisation in Bosnia and Herzegovina.

The data used in the study was made on the basis of the processed data of the Centre of Legal Assistance for Women Zenica (CPPZ) for the period of 01.01.2013. - 31.08.2014. During this period CPPZ has provided 2168 legal services, of which 68.54% were in the field of family law.

During the 20 months, violence through the internet and mobile telephony has experienced a total of 1,201 clients, or 55.40% - which is more than every second person.

Compared to the 12 months of 2012, where it was a one in four, we notice increase. We can't claim with certainty that this is a real increase, because part of it is the result of our office paying more attention and recording these details from the client statement.

Violence and harassment is mostly done via mobile phone (SMS), and in 760 cases. Harassment via facebook prof ile has recognized 400 clients, sta lking and threats over the Internet or a mobile phone 39, and tapping and recording 2 clients.

Often after threats were made virtually via SMS and facebook, abusers continued their harassment in person.

And during the 2013/14 year clients from urban areas were more exposed to harassment via the Internet, while clients from rural areas weren't exposed to this type of harassment, except threats made via text messages.

Clients who have experienced a variety of harassment via the internet are between the age of 27-45. We note also that younger women are more frequently and severely exposed tothe harassment via the Internet.

A common case is that after the relationship ends bullies "make" fake profiles of his former partner and bring them in inconvenient situation.

Case: spying via computer, unauthorized "intrusion" into the computer, espionage, psychological violence via photos.

The client contacted the Centre for Legal Aid over sister who asked some of us come to thecilents' apartment with to discuss and look at enhancements her husband used for a long time for spying. He was on a business trip, so it was feasible, and the client didn't dare to come in our office because she was afraid that someone will see her and if the husband found out, she could have an additional problem.

In this case I was on the site and saw the devices which her husband used because the she wasable to photograph and document it.

After detailed examination of the evidence conditions were filled for bringing criminal charges. However the client dropped all of this because she was frightened - her husband is celebrity in town and a former police officer.

End notes:

For each collected data in the fie ld of IT violence all cases from 2013 and 2014 had to be read in order to find the elements that are the focus of this study. Only a few months back data is recorded in the admission list of clients, and the search is partly easier. The intention is to adapt an electronic database in order for these indicators to be easier extracted in the future.

Dr Fiona Gray; Sarah Green[140]
Affiliation: RASASC – Rape and Sexual Abuse Support Centre; End Violence Against Women Coalition
Country: UK

5th August 2015

Re: Internet Governance Forum Best Practice Forum on the online abuse of women

We are responding to your call for case studies for the IGF good practice document in countering abuse of women online which was forwarded through to our organisations from our Government Equalities Office. Thank you for the opportunity to consult on this important issue.

Included with this response is a copy of the report by the End Violence Against Women Coalition which compiles the results of a roundtable held in July 2013 looking at the problem of online forms of violence against women in England. A short podcast of the discussion is still available online.[141]

The report, *New Technology, Same Old Problems*, reviews the different ways in which women and girls are abused online – from threats and harassment targeted at individual women, to the distribution of misogynistic and violent imagery and so-called 'revenge porn'. The report notes that government, police and schools in England are on the backfoot when dealing with these issues – for example not taking rape threats online seriously - and makes recommendations for change, including to social media companies.

Though the report is now almost two years old, we would still stand by the recommendations and are waiting for many of these to be implemented. These recommendations covered action from government, policy-makers, enforcement and prosecution, regulators and social media service providers. Below is an updated table on progress against these as at 1st Agust, 2015.

Recommendation	**Progress**
Technology and media, including new	Not yet implemented. We have recently had

[140] Note that in the interest of privacy, the contributors' email addresses and other personal details were omitted from the letter.
[141] See http://www.theguardian.com/technology/the-womens-blog-with-jane-martinson/audio/2013/jul/24/podcast-tech-weekly-women-digital-abuse.

media, should be fully integrated into the Home Office led VAWG strategy.	a new government in Westminster (May, 2015) and should be receiving a revised VAWG strategy in the Autumn.
The Department for Culture, Media and Sport should establish an advisory group on sexism and the media, including new media.	Not yet implemented.
The Government should ensure that all survivors of violence and harassment, whether online or offline, have access to specialist support services in their community.	Not yet implemented. Still uncommon to recognise need for support for women who have experienced online forms of VAWG.
There should be a legal obligation on all schools to teach respectful and consensual relationships, whether offline or online, in an age-appropriate way from primary school. This should be clearly linked to lessons on media literacy and technology.	Not yet implemented. Both our organisations and many others are involved in ongoing campaigning aimed at the new government to secure action on this recommendation. There is now a growing body of evidence and supporters that are lobbying for statutory sex and relationships education, including support from the Education Select Committee in February of this year.
Data should be published by the Home Office for each police force area on their rate of prosecutions and convictions for offences involving social media.	Partly implemented – some offences are being recorded. For example, new legislation was introduced in April criminalised the sharing of private, sexual photographs or films, where what is shown would not usually be seen in public (revenge porn). We expect to see this in the Office of National Statistics reporting statistics
Police and Crime Commissioners should include social media in local violence against women and girls strategies, including officer training and access to specialist support services in their area.	Unknown as the VAWG strategies of different PCCs are currently not analysed comparatively.
The Government should review whether existing laws adequately address	Partly implemented. Government consultation led to specific criminalisation

violence against women and girls that is carried out via social media.	of revenge pornography.
There should be a consistent approach to regulation of violent, sexualised, sexist, racist and other harmful imagery across the media.	Not implemented. Regulation is varied and inconsistent across media.
Media regulators such as the Advertising Standards Authority and Ofcom should adopt the same framework and 'harm' based criteria as the British Board of Film Classification.	Not implemented. Regulators other than the BBFC still operating on liberties not harm basis.
Social media companies should consult their users and experts about how to respond to violence against women and girls.	Partly implemented. Google announced in June 2015 it will honour requests to revenge porn images. Twitter introduced abuse/report buttons in August 2013 after a campaign from Caroline Criado-Perez (see report) and others. Onus still on campaigners lobbying for change rather than companies proactively consulting with their users.
Social media companies should work with women's groups to review their terms and conditions to ensure that they explicitly prohibit abuse and harassment, particularly of women and other targeted groups. Imagery that promotes abuse and violence, even where not targeted at a specific person, should be removed.	Not implemented.
Social media companies should work with the Department for Culture, Media and Sport to develop a best practice guide to tackling violence against women and girls on social media sites.	Not implemented.
Social media companies should commit to removing any intimate photograph from a site where the subject requests it, even where they are not underage and where the photo was taken with their consent.	As above, Google announced action on this in June 2015. No movement from other companies.

In addition to the above, the Government Equalities Office (GEO) commissioned the production of a central online portal providing advice on what action individuals, especially women and LGBT people, can take against offensive, damaging or threatening content online and in other media. The site has been developed by Galop,[142] in partnership with a number of specialist women's and LGBT organisations. The site is available at www.stoponlineabuse.org and we are currently involved in reviewing the content for the section on sexism.

Finally, we have attempted to add comments to the Google Drive document however have been fairly unsuccessful as with the existing comments it was difficult to ascertain what was to be included in the final document. It may be easier for us to provide comment – if needed in additional to this response - directly on a draft and then have these comments merged into the wider document if that would be possible.

I hope this short response is clear and helpful. Please do not hesitate to get in touch if you would like me to elaborate on any of it. I look forward to hearing about the next stage.

[142] Galop is London's leading charity for lesbian, gay, bisexual and transgender people http://www.galop.org.uk/

APPENDIX 4: THEMATIC ANALYSIS OF COMMENTS RECEIVED ON DRAFT II

1. Introduction

Draft II of the BPF's work was published on the IGF's review platform, an open platform that allows participants to leave comments on pages in their entirety, on specific paragraphs, or on other commentators' comments. Each IGF BPF published various drafts on this platform in order to gather community input on their work, and thereafter considered and/or incorporated the comments on the relevant draft as part of the iterative process BPFs follow. Thus subsequent drafts reflect, as far as possible, the input of commentators.

For Draft II of the BPF concerned, each commentator was required to use his or her name and email address when submitting a comment, although there was no way to verify the identity of commentators and/ or of knowing whether each commentator was unique. Commentators were able to provide input on Draft II for a period of 14 days, between 5 and 20 October 2015. Note that the timing of this comment period coincided with the BPF's social media campaign, which (for reasons explained in Appendix 5) led to a substantially higher number of comments (96 comments) than was the norm for input on other BPFs' draft documents.

2. Method

BPF participants decided that it was important to analyse each comment on Draft II and to provide reasons for the actions taken to address each comment. For this reason, thematic analysis was selected as a method to analyse all of the comments, as it allows one to identify, analyse and report patterns or themes in datasets in a lot of detail. It is also a flexible method that can be used independently of specific theories. The method provided a good a starting point for an analysis of the 96 comments received on Draft II on the IGF's dedicated online review platform; thus helping one obtain a better idea of what comments are significant to the BPF's work and how it can be incorporated into further draft documents.

3. Description of codes and related actions

After studying the comments received on Draft II on the review platform, nine common themes and/or classifications were identified. These themes relate to content, the BPF report's scope and mandate, methodology, technical aspects, and other themes. Explanations for each of these themes are provided below, along with the actions taken to address each theme. In the subsequent section, each comment is coded and the relevant action is explained and expanded upon where necessary.

Content

Code 1: Comments recommending new additions and specific changes to the contents of document. These comments are not defined in other codes, and do not relate to structure, style, spelling or punctuation (see Code 7 below, which relates to structure, style, spelling or punctuation).

Action 1: Specific notes detailing inclusion/ not are included in 'action/ notes' columns in section 4.2 of this Appendix below.

Code 2: Comments pertaining to definitions (including comments calling for clearer definitions of the problem, and disagreements about what constitutes abuse/ violence). Does not include comments to the effect that there is no such thing as online violence or abuse, or that offline violence/ abuse is more important to address than online violence/ abuse (see Code 4 below).

Action 2: Clarify reasons for including examples of definitions from other reports and legislative instruments; the need for flexibility in definitions of the problem; the need for including examples of behaviour that might constitute abuse and/or violence; and the importance of acknowledging different contexts. Define and differentiate between the terms 'violence' and 'abuse'.

Code 3: Comments about balancing women's rights with other fundamental rights (e.g. how freedom of expression is impacted by anonymity prescriptions, and comments related to fears that governments might use measures to protect women online as excuses for effectively limiting other rights).

Action 3: Emphasize the importance of balancing rights and reinforce BPF's understanding that rights are intertwined: without ensuring the respect for women's rights online and the prevention of online violence/ abuse against women, other fundamental rights (like the right to freedom of expression) are also violated. By detailing effective practices for protecting women online, the BPF's work therefore bolsters work to promote other fundamental rights, like freedom of expression, online.

Scope and mandate

Code 4: Comments about the scope and mandate of the BPF's work (including comments to the effect that there is no such thing as online violence/ abuse; that the BPF should rather focus on violence/ abuse in the 'offline'/ non-cyber world; and/or concerns about why the report does not consider the online abuse of men). Does not include comments relating to definitions, including the difference between violence and abuse (see Code 2 above).

Action 4a: Include explanation for why the BPF's work focused on primarily women and girls. Include recommendation for future research to investigate incidence of abuse against men online, and appropriate remedies. Commentators referencing Pew research's *Online Harassment* study (2014)[143] to argue that men are more likely to be abused online than women are reminded of the other findings of the Pew research report: while men are more likely to experience name-calling and embarrassment (or what the report calls 'less serious' forms of abuse), young women are 'particularly vulnerable to sexual harassment and stalking' (what the report calls 'severe' forms of abuse). In addition, the research was done using a survey administered on a randomly selected panel of only U.S. adults who self-identify as Internet users (representing 89% of U.S. adults). In other words, the findings are representative only of a U.S. population.

Action 4b: Emphasize, with reference to relevant research, the need to address online violence/ abuse. Clarify that by investigating online abuse/ violence, the BPF is by no means trivialising 'offline' violence/ abuse. Commentators are furthermore referred to examples in report of online violence/ abuse, which emphasize the consequences of such abuse/ violence and indicate the importance of addressing such incidents.

[143] Pew Research (2014), *Online Harassment.* Available online: http://www.pewinternet.org/files/2014/10/PI_OnlineHarassment_72815.pdf.

Code 5: Comments indicating a confusion of the report with the Broadband Commission report *Cyber Violence against Women and Girls: A world-wide wake-up call* (2015), including comments that criticize references to the 'withdrawn' report.

Action 5: Explain that Draft II was published after the Broadband Commission's report was published, but before it was withdrawn (although it is still 'published' and remains accessible online). Include a note explaining that the Broadband Commission's report is currently being updated and will likely be published before the end of 2015. Update relevant sections when updated report is published.

Methodology

Code 6: Comments related to research methods used (including comments about the survey).

Action 6: Ensure that methodology, specifically in relation to survey, is clearly defined. If necessary, explain nature and objectives of survey to commentators again, including nature of population and sample (and sample size). Commentators referencing Pew research's *Online Harassment* study (2014)[144] are reminded of the other findings of the Pew research report: while men are more likely to experience name-calling and embarrassment (or what the report calls 'less serious' forms of abuse), young women are 'particularly vulnerable to sexual harassment and stalking' (what the report calls 'severe' forms of abuse). In addition, the research was done using a survey administered on a randomly selected panel of only U.S. adults who self-identify as Internet users (representing 89% of U.S. adults). In other words, the findings are representative only of a U.S. population.

Technical

Code 7: Comments relating to style, grammar, spelling and citations, but not relating to the contents of the document (see Code 1 above).

[144] *Ibid.*

Action 7: Specific notes detailing inclusion/ not are included in 'action/ notes' columns in section 4.2 below.

Other

Code 8: Comments that are not constructive and/or helpful to improve the BPF's work, including spam and those related to #TBTT.

Action 8: Commentators invited to contact BPF for constructive dialogue/ to participate in process, and reminded that the BPF has always followed an open, inclusive and transparent process and that all commentators are welcome to participate and contribute to the BPF's work as long as they do so in accordance with the IGF's Code of Conduct.

Comments that were not coded:

- One comment on another comment; not on contents of report.
- One attempt to provide feedback on survey, which is closed.

4. Results

4.1 Summary of comments

In total, 36 commentators participated and 96 comments were collected (although one was not accepted for the use of language that does not adhere to the IGF's Code of Conduct). While most commentators only left one to two comments, one commentator left 24 comments. In the table below, the prevalence of themes in relation to the number of codes given in total is summarised (as some comments received more than one code).

Code	Short description	Prevalence
1	Comments recommending new additions and specific changes to the contents of document	**27%**
2	Comments pertaining to definitions	**13%**
3	Comments about balancing women's rights with other fundamental rights	**7%**
4	Comments about the scope and mandate of the BPF's work	**20%**
5	Comments indicating a confusion of the report with the Broadband Commission report	**2%**
6	Comments related to research methods used	**3%**
7	Comments relating to style, grammar, spelling and citations	**17%**
8	Comments that are not constructive and/or helpful to improve the BPF's work	**11%**

4.2 Comments, codes and actions

In the section below details of every commentator (or the identity given), the paragraph concerned, the comment (verbatim), the code given to the comment (i.e. the theme(s) identified in the comment), and the relevant action taken is listed and explained (where necessary). The tables are divided into four categories: a) Editors' note; b) Part 1: Introduction and Methodology; c) Part 2: Results; and d) Part 3: Appendices.

a) Editor's note (9 comments):

Name/ email/ date/ IP	Code	Para/ section/ heading concerned	Comment (verbatim)	Action/ notes
johnnynumeric johnnynumeric@gmail.com	8	**Para 4** This is the second draft document ('Draft II') produced by a community of	Why is it you openly invite constructive dialouge, yet when approached with valid criticism you refuse to debate, and yell "harassment"? Your agenda has been exposed. TRIPLE	Action 8

Submitted on 2015/10/17 at 4:44 am		participants….	WEASEL WHOPPER	
Mohit Saraswat immohit4u.blogspot.ae/ x mohitsaraswat@gmail.com 86.97.90.155 Submitted on 2015/10/16 at 8:10 pm	4	**Para 9** The IGF provides a unique platform for the collaborative work of this BPF, which aims to collect the views of the broader Internet governance community on the topic of how to counter online violence against women and girls….	While not undermining the issue and sound biased; I think, it will be not a great idea to generalize online violence on sexual terms and leave big part of male population.	Action 4a
Ana Kakalashvili anna.kakalashvili@gmail.com mailto:anna.kakalashvili@gmail.com109.234.119.52 Submitted on 2015/10/17 at 2:04 am	1	**Comment on whole page**	The first thing that should be made here is to defining the word "gender" and what is meant by it. The second issue I would like to like to raise is about safe IG environment, which isn't related to harassment online, but it concerns in-person participation of females at Internet Governance events and in the IG sphere in whole. While we are aware that this sphere is dominated by male representatives, there is a high chance (and not publicly/officially known facts) of harassment. It is crucial to assure that the IG atmosphere at the actual meetings is free from harassment. This way, female representatives would be more encouraged to participate. If actual harassment acts won't be eliminated at IG events, this would most probably mean another drop in the number of female representatives. A network of IG female representatives should be	Action 1: While comment is not incorporated into document, topic is highlighted at BPF meeting to discuss relevance to BPF session at IGF 2015. Participant is pointed to variety of workshops at IGF 2015 that deals with the issue of improving gender participation at IGFs.

			established, so that females could be able to support, advice, encourage and empower each other.	
Russell russell.holgate@gmail.com 184.147.2.221 Submitted on 2015/10/14 at 7:00 am	4	**Comment on whole page**	I agree that threats of violence are an issue on the internet, but it is NOT A WOMEN'S ISSUE. The threats happen to EVERYONE and are so rarely carried out that those on the receiving end can go about their daily lives unhindered. There is no such thing as online violence, i.e. you cannot physically harm someone over the internet, but by supporting this idea of online violence, of countering online violence and of it being specifically a women's issue, you're allowing people and groups of people to be shamed with false accusations, unchallenged. I strongly urge the UN, who rightfully respects amnesty and equality, to question if by trying to solve issues of sexism, they aren't creating them.	Action 4a & 4b
d denryuushield-poop@yahoo.com 137.151.174.128 Submitted on 2015/10/12 at 6:28 pm	4	**Comment on whole page**	This entire article and initiative hinges on obsessing over the incredibly pitiful "violence" that is people saying mean things on the internet t0 women, and ignoring not only that exact same abuse directed at men but the endless mounds of actual violence in actual real life directed at both genders you could be addressing. I mean, could you at least be wanking over actual real-life violence against women? It'd still be a useless, redundant action ignoring the endless streams of physical and sexual violence directed towards men by both men and women that are never addressed, ever, but at least you'd actually be accomplishing some tiny sliver of something.	Action 4a

ty2010 ty2010@aim.com 184.17.194.57 Submitted on 2015/10/09 at 7:12 am | In reply to tehy.	4	**Comment on whole page**	So men can be doxed and employers/landlords harassed until they're out of a job and home for disagreeing. I see nothing coming of this except extending the open season on men. There are many others besides Tim Hunt and their stories are rarely told. The offline affects are what needs dealt with.	Action 4a
George Orwell BigBrother@1984.com Submitted on 2015/10/09 at 3:52 am	8	**Comment on whole page**	War is Peace! Freedom is Slavery! Ignorance is strength! Big Brother (The UN) is watching you! It is not enough to obey, you MUST LOVE BIG BROTHER!	Action 8
Thoth thoth@pymid.com 174.52.102.92 Submitted on 2015/10/09 at 3:18 am	8	**Comment on whole page**	No. To all of it. Want to help women? Help the men in their lives to protect them. Men can take it. They have for thousands of years. But they need a reason. Treating the men like children won't help. Treating the women like children won't help. So no, to all of it.	Action 8
tehy	8, (3)	**Comment on whole page**	I'm so glad at the wonderful work you're all doing here; I	Action 8, (3)

y.aboody@outlook.com 76.91.3.204 Submitted on 2015/10/08 at 6:10 pm			would hate to think that sucky liars could be called out for such on the internet if they happened to have a Vagina. Make sure to suppress all rational thought! Wouldn't wanna miss any!	
Bobby Snider yditys@gmx.co.uk Submitted on 2015/10/16 at 2:15 pm	8	**Comment on whole page**	A quote from our dear friend… "Tyler The Creator": Hahahahahahahaha How The Fuck Is Cyber Bullying Real Hahahaha Nigga Just Walk Away From The Screen Like Nigga Close Your Eyes Haha	Action 8. Note that this comment was not 'accepted' for failure to adhere to the IGF's Code of Conduct. This is the only comment that was not accepted.

b) Part 1: Introduction and Methodology (26 comments)

Name/ email/ date/ IP	Code	Para/ section/ heading concerned	Comment (verbatim)	Action/ notes
Bryanna Hatfield Temprence2@live.com 107.77.89.46 Submitted on 2015/10/17 at 6:20 am	8	**Comment on whole page**	We are not your shield to continue using females as ur backbone is straight up #Takebackthetech #Wearenotyourshield	Action 8

Anon13 tilltoger@gmail.com 45.46.83.138 Submitted on 2015/10/11 at 7:07 pm	4	**Comment on whole page**	The problem of harassment of women and girls is only a problem if it is occurring dramatically MORE than the harassment of men and boys, and there's no evidence of that provided (and in fact the stats I've seen say it isn't true). If the position is that women and girls being harassed is a unique crisis even if men and boys are harassed just as much, the take away is either that women and girls need special protection because they can't take care of themselves, or that the suffering of males isn't as important.	Action 4a
Jay jaypesci@hotmail.com 86.26.5.242 Submitted on 2015/10/11 at 2:26 am	4, (3)	**Comment on whole page**	There is absolutely no mention of men and boys being targeted by online abuse ANYWHERE in this document, despite the fact that they receive MORE abuse than women online. Why not make this document gender-neutral? You will likely be MUCH more successful in taking away everyone's right to free speech if you do. Just a thought.	Action 4a
Fran Mambles benqd86@gmail.com 64.92.27.6 Submitted on 2015/10/09 at 7:24 am	5, (8)	**Comment on whole page**	So nobody finds it odd that we're just gonna push an act based solely on here say and conjecture or the contents of one's hard drive? Nobody? Nobody at all? Seriously? Jesus, U.N. you are screwing up big time.	Action 5, (8)

David Lillie Dreamkeeperscomic@gmail.com 71.227.103.147 Submitted on 2015/10/11 at 7:34 pm	2, 4, 5	**Para 3** *'… 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."*	This goal is too broad to be effectively handled by a single directive. Human trafficking, child pornography, and other sexual crimes are entirely distinct from such concerns as "Cyber Violence," which has been defined so broadly as to encompass potentially any casual dissent or online socialization. Conflating "Cyber bullying" and "Online Violence" with human trafficking and child pornography, and prescribing the same solutions to each situation, is ludicrous. For this report to avoid the due mockery drawn by its predecessor, it must narrow the scope of it's objectives and refrain from convoluted attempts to equate violence with the subjective "psychological harm" of twitter disagreements.	Action 2, 4b, 5
Ashell Forde ashell.forde@gmail.com Submitted on 2015/10/16 at 8:41 pm | In reply to David Lillie.	4	**Para 3 (above)**	David, I have to disagree with you. These issues all seem to disproportionately affect women and girls online and the concept of cyber violence should not be dismissed as "entirely distinct" from the real world harm that is caused by online actions.	Other [Comment on another comment; not on contents of report]

			I did not interpret the statement to in any way conflate cyber bullying with human trafficking/child pornography. It simply calls on governments to develop mechanisms to combat a wide range of harmful uses of ICTs, not that all these behaviors are the same. Also, the use of the word "mechanism**s**" would suggest that different methods of combating these behaviors could be developed.	
Shreedeep Rayamajhi womenoutcry.blogspot.comx weaker41@gmail.com 113.199.141.85 Submitted on 2015/10/16 at 7:42 pm	1, 2	**Para 3 (above)**	I think the problem cannot be solved by just having a definition but there should be a point of setting standards in terms of the basic core values. I seriously think today's women get abused online not because they are scared or they do not know the reality but they are unknowingly fall pray to vulnerabilities or they create sub standard situation failing to understand the right of privacy and being too unsafe on internet. So at first the core values of internet in terms of privacy and other values should also be well defined so that it helps them to understand their vulnerabilities. Just by creating solution, you cannot understand the problem to understand the problem you have to root the problem and to root the problem you have to understand their values and mentality and it is utmost important.	Action 1: The importance of raising awareness and understanding underlying issues that contribute to human rights violations online was stressed in numerous sections of the report. In addition, include a separate section on human rights and interests and developments pertaining to a

				'constitution for the Internet' (see Part I D i)
Ian Bibby ibbibby@yahoo.com 73.163.2.25 Submitted on 2015/10/11 at 12:01 am	2, 7	**Para 4:** While great strides have been made to improve connectivity and Internet access around the world, resulting in increased opportunities for advancing rights and interests of different sections in society, increased access has also resulted in the use of technology to perpetrate acts of abuse and violence against women and girls (VAWG). Online VAWG has increasingly become part of women's experience of violence and their online interactions; encompassing acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs) such as telephones, the Internet, social media platforms, and email. Examples of online VAWG include (but are not limited to) online harassment, cyber stalking,	As it stands, this paragraph is incoherent, and will cause people to tune this report out. For instance, it's surely stretching the definition of words to literally call misogynistic speech a form of violence. If speech that insults women is violence against women, then doesn't ALL insulting speech have to be violence against whoever or whatever is being insulted? Surely this report doesn't mean to imply that all mean words on the Internet are violence. The same goes for online blackmail. How can online blackmail be considered violence when offline blackmail isn't? I believe the entire premise of this report, that all bad behavior online is tantamount to violence (which is illegal) needs to be reassessed and replaced with more defensible tack.	Action 2 Action 7: Changed footnote that is linked to cited examples: "Note that these examples do not always constitute abusive and/ or violent actions. See Section C below for a detailed analysis of the types of actions that may, under certain circumstances, constitute online violence/ abuse."

		misogynistic speech, privacy invasions with the threat of blackmail, viral 'rape videos' that force survivors to relive the trauma of sexual assault, and the non-consensual distribution of 'sex videos' (see Section C below for definitions).		
Morgan Qualls j.morgan.qualls@gmail.com 108.227.108.71 Submitted on 2015/10/12 at 1:46 am	2, 4	**Para 4 (above)**	Speech and communication are categorically separate from violence, the latter of which entails physical, corporeal force. Communication can be used to threaten violence, or heighten the psychological impact of separately performed violence, but communication itself in isolation cannot constitute violence. Abuse of terminology in this fashion is at best disingenuous and at worst trivializes and dilutes discourse about actual violence.	Action 2; 4b
John Smith mountainofdestiny@yahoo.com 166.70.207.2 Submitted on 2015/10/11 at 6:59 am	4	**Para 4 (above)**	In the interests of honesty, it might be worth noting in this paragraph or nearby that Pew Research has established that men and boys are statistically more likely to suffer online harassment than women and girls. Not noting that online harassment against women and girls is a minority of such incidents implicitly misrepresents the issue. See the study here	Action 4a
J. Carl Henderson	2	**Para 4 (above)**	People disagreeing with someone is not "online	Action 2

j.carl.henderson@gmail.com 72.64.98.120 Submitted on 2015/10/19 at 9:07 pm			harassment", but too many people seem to think it is. Additionally, "misogynistic speech" is extremely subjective, and culturally linked. Using these as an examples of abuse or violence is nonsensical.	
Shreedeep Rayamajhi womenoutcry.blogspot.comx weaker41@gmail.com 113.199.141.85 Submitted on 2015/10/16 at 7:59 pm	1	**Para 4 (above)**	It is so true that specially for the underdeveloped countries internet has been passed on without any preparation and its very vulnerable, the reach and access has become a problem for VAW in many cases. But there is the role of the government and various stakeholder in terms of safeguarding the public by making proper policies and developing core value The main problem here is difference of mentality and understanding as in the western society nudity is considered normal but in eastern society there is a huge misconception regarding nudity and skin. so the lack of understanding creates a difference. Even for young girls the trend of releasing a self nude selfie has been a trend where they do it without know the consequences. They do it because their friends are doing it.	Action 1: Stressed importance of raising awareness and understanding and addressing underlying issues, especially in diverse cultural contexts. Include quotation from comment in Part I.

			This is the mentality that we need to break	
Ian Bibby ibbibby@yahoo.com 73.163.2.25 Submitted on 2015/10/11 at 12:11 am	4	**Para 5:** Online VAWG can, among other things, limit women's ability to take advantage of the opportunities that ICTs provide for the full realisation of women's human rights, often violate women's human rights, and reaffirm and reproduce gender stereotypes. Online VAWG is aggravated by various obstacles that prevent women from exercising their right to access justice in both online and offline environments, including a lack of effective and timely remedies to address online violations experienced by women, and obstacles faced in collecting evidence relating to online VAWG	The part about reaffirming or reproducing gender stereotypes should probably be removed. It conflicts with the main thrust of this report that women are emotionally weaker and more vulnerable than men, and that online harassment of women is therefore a bigger problem than online harassment of men (which as this report's sources show is more common than harassment of women) and more likely to intimidate women into not taking advantage of the opportunities that ICTs provide.	Action 4a
Lianna Galstyan lianna@isoc.am 149.13.247.10 Submitted on 2015/10/08 at 2:57 pm	7	**Para 6:** Over the past six years, increasing attention has been paid to understanding the nature, harm and consequences of online VAWG against women by the	In the first sentence after VAWG I suggest to remove 'against women' as VAWG already indicates that.	Action 7: Effected change in full.

		media, governments and women's movements. This is evidenced in the formal recognition of online VAWG in significant women's rights policy spaces and the focus on secure online practices for women and women human rights defenders.		
Courtney Radsch cradsch@cpj.org 73.163.29.66	1	**Para 6 (above)**	"the media" makes no sense here – media are either inanimate objects (as in the medium or communication) or media refers to a range of actors and this should be specified because lots of different actors use "the media" including governments. So does this refer to media outlets? journalists? bloggers?	Action 1: Effected change in part: "…by the media (including journalists and citizen journalists)".
Ashell Forde ashell.forde@gmail.com Submitted on 2015/10/16 at 8:49 pm	7	**Para 6 (above)**	"…harm and consequences of online VAWG [against women] by the media…" The bracketed portion of this sentence is redundant.	Action 7: Effected change in full.
Conor Rynne conor.rynne62@gmail.com 86.16.177.74	1, 4	**Para 7:** But the concern of online VAWG has arguably not been adequately taken up by the various stakeholders within the	Citation needed. There are plenty of examples where social media have actively taken action regarding internet abuse. Also, it is physically impossible to commit violent acts over	Action 4b Action 1:

Submitted on 2015/10/11 at 2:32 am		Internet governance ecosystem. There is still a lack of awareness regarding what kinds of online conduct constitute abusive and violent behaviour and the variety of actions that can be taken to address and prevent such behaviour in the future.	the internet, as an act of violence requires physical force.	Defined 'Internet governance' in Interpretation Notes section and in paragraph concerned to clarify difference between governance actors and steps taken by social media platforms.
Conor Rynne conor.rynne62@gmail.com 86.16.177.74 Submitted on 2015/10/12 at 1:34 am | In reply to David Lillie.	4	**Para 7 (above)**	Insulate the report from sexism? The report is sexist to it's very core. Research has proven that men catch similar amounts of online abuse to women, but this report is all about protecting one gender. There is no evidence, none at all, that says women suffer from this more than men, only sensationalised reports in the media.	Action 4a
David Lillie Dreamkeeperscomic@gmail.com 71.227.103.147 Submitted on 2015/10/11 at 7:39 pm	4, 1	**Para 7 (above)**	For it to effectively protect all women, VAWG must apply to everyone- even, potentially, men. Anonymous accounts that choose to withhold gender information deserve the same protections as those who	Action 4a Action 1: Included paragraph regarding protection of

			choose to make their gender public. Additionally, establishing objective standards of conduct- what is acceptable behavior, and what is not, regardless of gender- will insulate this report from accusations of sexism.	anonymous accounts. Consider including section on core values, or a 'constitution for the Internet' as part of the recommendations.
Conor Rynne conor.rynne62@gmail.com 86.16.177.74 Submitted on 2015/10/11 at 2:37 am	4	**Para 8:** Taking effective action to counter the growing phenomena of online VAWG is not only important in ensuring that the Internet fulfils its potential as a positive driver for change and development, but also in helping to construct a safe and secure environment for women and girls in every sphere of life.	Internet abuse is a growing problem faced by **both** genders. To paint it as a women-specific issue, or that the consequences only happen when a woman is the victim is grossly dishonest. Source: http://www.pewinternet.org/2014/10/22/online-harassment/	Action 4a
V.Z. streptococcus.viridans@gmail.com 80.220.78.108 Submitted on 2015/10/13 at 11:59 pm | In reply to C Rynne.	4, 6	**Para 8 (above)**	It is not only grossly dishonest, but it also presents only two possible conclusions: Either the males experiencing the same kind of issues are so much less important that they fall out of relevance, or The females cannot handle those issues the same way the males do. Both of which are sexist in the highest order. In addition to this, the findings in your linked study regarding the outcomes of online harassment go counter to	Code 4a; 6

			the findings in this report: First we have to acknowledge the difference in sample size: the pewinternet.org study states their sample size being 2839, while this report declares its number of survey respondents to only be 56: http://review.intgovforum.org/igf-2015/best-practice-forums/draft-ii-bpf-on-practices-to-counter-online-violence-against-women-and-girls/part-3/#pAtnorwcwtlpsbrwitapcssgasftcIsbnhtgnnmeOtsatowvtpgduie The pewinternet.org study reports the after-effects of online harrasment to be very different from what is stated in this report with only 28% of respondents finding their experience “extremely” or “very” upsetting; 21% reporting a “somewhat” upsetting outcome and **52%** responding that their experience was only “a little” or “not at all” upsetting. This goes to highlight that though there is a significant minority of respondents that had a very upsetting experience, the majority did not rate their experience as significantly upsetting. To me — based on the aforementioned points — the language used in this report is overstating the severity of the problem and is misguided in labeling those issues as A gendered problem; Violence and not harassment;	

Lianna Galstyan lianna@isoc.am 149.13.247.10 Submitted on 2015/10/16 at 10:55 pm	7	**Para 19:** Addressing online VAWG requires considerable cooperation and input from a multitude of stakeholders, including the technical community, private sector, civil society advocates, organizations, governments, international organizations, the academic community, users, and young people.	There is no need to mention organizations, then international organizations. Either to remove one of them, or international is meant here intergovernmental organizations maybe?	Action 7: Omitted first mention of 'organizations'.
Lianna Galstyan lianna@isoc.am 149.13.247.10 Submitted on 2015/10/16 at 10:58 pm	7	**Para 27** Solutions, responses and/or strategies to counter online abuse and violence against women and girls – to identify existing policy and other measures; highlight common practices that have proven to be effective; and to investigate the consequences of policy interventions	add full stop at the end of the sentence	Action 7: Effected change in full.
Maria Paola Perez https://ve.linkedin.com/in/paoperezcx paoperezc14@gmail.com 186.89.70.108 Submitted on 2015/10/11 at 7:10 am	1	**Para 41:** Due to the nature of the Internet as a distributed network of networks, addressing online VAWG requires considerable input and cooperation from a multitude of stakeholders, including the technical community, private sector, civil	I know that all the stakeholders cooperation is required. But the key that must exist between the stakeholders is the trust to focus on our common problems.	Action 1: Highlighted need for trust amongst stakeholders in Part II paragraph 18.

		society advocates and organizations, governments, international organizations, academic community, users, and young people.		"Addressing online VAWG requires considerable cooperation and input from, and trust among, a multitude of stakeholders…."
Encel Sanchez encels@gmail.com 186.188.121.198 Submitted on 2015/10/16 at 11:28 pm	6	**Para 44:** In March 2015 a wide call was issued to the IGF mailing list to encourage participants to join BPF mailing lists, including this one (see Part 3, Appendix 3 for the call). The coordinators also directly contacted individuals from various stakeholder groups to encourage participation. Stakeholders were invited to participate in fortnightly virtual meetings, by commenting on and visiting an online platform hosted on the IGF's website, and by following discussions on the dedicated BPF mailing list.	In addition to the invitation to mailing lists, it's should be to follow up on the topics of discussion and perhaps provide more specific sub-lists.	Action 6: Added sentence clarifying that follow-up on topics was done using mailing list in Part II paragraph 20. "Where necessary, the mailing list was also used to send follow-up emails to elicit responses and to stimulate debate on specific topics, and social media platforms like Twitter and

				Facebook were used to elicit responses to the survey and other case studies."
Maria Paola Perez https://ve.linkedin.com/in/paoperezcx paoperezc14@gmail.com 186.89.70.108 Submitted on 2015/10/11 at 7:14 am	1	**Para 51:** A total number of 56 survey responses were collected, with the largest proportion of responses submitted by respondents who identified themselves as part of the civil society stakeholder group (41%), and the smallest number from the technical community (4%)…	We need more technical community in this issues. Im technical and I was violence victim. Is a problem that could affect every women.	Action 1: No change in document, but emphasize importance of technical community participation in panel at BPF session at IGF 2015. Invite member from ISOC to provide input from technical community on panel.
Encel Sanchez encels@gmail.com 186.188.121.198 Submitted on 2015/10/16 at 11:31 pm	1	**Para 61:** To raise more awareness of the importance of the issue, and to gather responses in respect of some sections of the BPF's proposed scope of work, a social media campaign was planned for mid-	The spread through social networks is important to use communication tools such as Twitter and Facebook can help.	Action 1: Added sentence clarifying that follow-up on topics was done using mailing list and

		October.		social media platforms in Part II paragraph 22. "Where necessary, the mailing list was also used to send follow-up emails to elicit responses and to stimulate debate on specific topics, and social media platforms like Twitter and Facebook were used to elicit responses to the survey and other case studies."

c) Part 2: Results (57 comments)

Name/ email/ IP/ date	Code	Para/ section/ heading concerned	Comment (verbatim)	Actions/ notes
Anon13	2, (1)	**Para 3:** Due to a lack of awareness of the types of	Your definitions of abuse are far too broad. For example, it is nearly impossible to conduct a proper	Action 2

		behaviour and/or conduct that constitute violence or abuse against women in an online environment, it is important to clearly define such conduct, with enough room to allow for its changing expression with technological development that affects new ways of interaction and potential violations.	political campaign against (or investigative reporting into) a female politician without monitoring them, collecting information, soliciting unwanted contact or attention, or presenting information that may damage their reputation. The easy answer is that exceptions should be made for public figures, but of course the problem with that in a social network age is identifying who counts as a public figure and who does not. A person with no official standing as a public figure may nevertheless shape the opinions of thousands or millions of people via social or political commentary on various outlets.	Action 1: No action.
Ashell Forde ashell.forde@gmail.com 104.153.134.131	7	**Para 5:** Online violence forms part of offline violence and abuse, and thus frequently permeates the offline sphere and extends from offline environments into online environments. For many women who experience online abuse from a partner or ex-partner, for instance, online abuse often forms part of a pattern of abuse that was also experienced offline, like ongoing domestic abuse…	I would agree with MORGAN QUALLS that this paragraph is more wordy than it needs to be.	Action 7: Effected change in part: "Women may experience online abuse that is concurrent to and related with physical abuse and/or violence."
Morgan Qualls	7	**Para 5 (above)**	This paragraph is a crime against the English	Action 7:

j.morgan.qualls@gmail.com 108.227.108.71			language. Strike it and replace with the sentence "Women may experience online harassment that is concurrent to and related with physical violence, for example as in cases of domestic abuse."	Effected change in part: "Women may experience online abuse that is concurrent to and related with physical abuse and/or violence."
J lcxbyyee@sharklasers.com 68.181.252.5	4, (1)	**Para 6:** There is a serious lack of awareness about women's rights and the impact of online VAWG on women's rights, as is also indicated by the survey results…	You've yet to demonstrate *any* significant impact that "online VAWG" has on women's rights–or that it has a somehow worse impact on women's rights than men's rights, gay rights, or any other group's rights. This is unadulterated presuppositionalism. It's *been decided* that this is a horrible problem and then you go on to say that it's a problem that people have no awareness of this problem. And since you've gone all-out for the VAWG narrative, rather than an online "violence" in general narrative, you've got to prove that VAWG is uniquely and unilaterally worse than online "violence" in general.	Action 4a Action 1: Rephrased section to clarify: "There is a lack of awareness of and respect for women's rights and the impact of online VAWG on specifically women's rights, as is also indicated by the survey results."
Ashell Forde ashell.forde@gmail.com 104.153.134.131	7	**Para 11:** Many of the examples of online abuse and violence (discussed in more detail below) cited by survey respondents were similar or overlapping (especially when	"Some respondents also felt that excluding women from [the] accessing the Internet…" The bracketed portion of the above sentence should be removed.	Action 7: Effected change in full.

		synonyms are considered)….		
Morgan Qualls j.morgan.qualls@gmail.com 108.227.108.71	3	**Para 11 (above)**	Denying access to technology on the basis of sex is patently an example of a human rights violation. It does a disservice to any affected populations to conflate violation of rights with "damaging reputation and/or credibility", which can be an outcome of legitimate political speech. A UN imprimatur on such equivocation would be unwelcome rhetorical ammunition for repressive regimes worldwide.	Action 3: Deleted the word 'online': "Some respondents also felt that excluding women from accessing the Internet and/or certain online services because they were female amounted to abuse."
Ashell Forde ashell.forde@gmail.com 104.153.134.131	1	**Para 13/14:** *i) Infringement of privacy*	In the final bullet point: Why only the victim's children? Why not her family, friends or coworkers?	Action 1: Reworded section to add suggestion: "…contacting and/or harassing a user's children, extended family, colleagues (etc) to gain access to her."
J lcxbyyee@sharklasers.com 68.181.252.5	2, 4	**Para 13/14 (above)**	It's also redundant. If this stuff is *not* innocuous, it would be better handled by a general act. Literally nothing in this list is unique to women, but the IGF is acting like they all are. And a decent amount of this (hacking, for example) is *already* illegal just about everywhere.	Action 2; 4a

Maria Paola Perez https://ve.linkedin.com/in/paoperezcx paoperezc14@gmail.com 186.89.70.108	1	**Para 13/14 (above)**	I have a doubt… This is independently of the person who infringement privacy of a women? I mean, we can consider violence against of woman if all of this issues has been made from other woman?	Action 1: Included new section on victims and perpetrators: Part I B ii.
John Smith mountainofdestiny@yahoo.com 166.70.207.2	4, 1	**Para 13/14 (above)**	Many of the behaviors in this list, both in this paragraph and in the others, are totally innocuous in the vast majority of instances in which they occur. For example, according to this report and its fundamental thesis that online harassment (defined as including all of the behaviors on this list) is "cyberviolence" and thus the equivalent of physical violence in terms of harm, if a parent took a picture of her daughter and then posted it to the family Facebook page, she would be guilty of abusing the daughter to the same extent as if she had punched the daughter in the face. Similarly, if a mass e-mail advertisement firm sent an e-mail to a woman without her express solicitation, that would be of similar seriousness to them sending a person to her door to physically attack her. Think about that and reflect on whether that is really an argument you feel comfortable making. If it is not what you want, consider adding a mens rea requirement to these factors. For example, state that these acts must be done with some kind of malice.	Action 2 Action 1: Consider recommendation to include an intention/ mens rea requirement.

J lcxbyyee@sharklasers.com 68.181.252.5	4, 2	**Para 17/18:** *iii) Damaging reputation and/or credibility*	Why is this unique to the Internet? Why is a resolution that deals with cyber libel/defamation necessary when we already have laws against these in most countries? Even the somewhat decent ideas in here are unforgivably redundant.	Action 4b, 2
J. Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	4, (3)	**Para 19/20:** *iv) Harassment (which may be accompanied by offline harassment)*	This section is a mess. By conflating clearly illegal actions, with legal but rude actions, normal political discourse, and pornography/erotica under "harassment" you appear to be attempting to to delegitimize speech you disagree with, or which offends your particular religious beliefs. Additionally, the many of the items on your "harassment" list are so subjective, that a bad state or corporate actor, could easily use this list as a handy means of suppressing dissent.	Action 2, (3)
William C. Johnson crashing00@gmail.com 72.23.81.128	2, 5, 3	**Para 19/20 (above)**	Most items on this list are so subjective, ill-defined, or non-specific that virtually any piece of communication on the Internet could be construed in such a way as to violate any or all of them. Who decides, for instance, whether a piece of online content portrays a woman as a sexual object? There are certain commentators who would put, for	Action 2, 5, 3

			example, virtually every video game ever developed into that category — therefore making this document what is effectively an interdict against that entire industry. I submit to the United Nations that it needs to solicit more input from people who understand the philosophical basis of free speech and the perils of introducing arbitrary and ill-defined constraints such as these before it again goes off half-cocked and releases another illiberal and poorly-researched travesty of a report.	
Ferreira twinzam.v@gmail.com 109.51.214.75	4	**Para 21/22:** *v) Direct threats and/or violence*	I dont understand why only the trafficking of women needs to be stopped. Technology is also used to alure men to work as slaves or as guinea pigs. One important point is that sexual assault isn't exclusive to women, men can also suffer from it with twisted results from violence and sodomy.	Action 4a
J lcxbyyee@sharklasers.com 68.181.252.5	4	**Para 21/22 (above)**	Beating a dead horse, but is it cool to traffic boys, then?	Action 4a
J. Carl Henderson j.carl.henderson@gmail.c	2,1	**Para 23/24:**	The trouble with including online "mobbing" here if someone says something controversial, it is quite	Action 2

om 72.64.98.120		*vi) Targeted attacks to communities*	reasonable to assume other people will respond with disagreement. The more high profile the person, and the more controversial the speech, the more people who will disagree.	Action 1: Clarified section as follows: "mobbing, specifically when selecting a target for bullying or harassment by a group of people, rather than an individual, and as a practice specifically facilitated by technology."
Ashell Forde ashell.forde@gmail.com 104.153.134.131	7	**Para 25:** *vii) Limiting women's access and/or use of technology*	"*Limiting women's access [to] and/or use of technology*" The bracketed portion should be included.	Action 7: Effected change in full.
J. Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	2, 1	**Para 27/28:** *viii) Theft or abuse of intellectual property*	1) Is there any reason to believe that women are disproportionately affected by IP theft? 2) "Ideas" are not protected as IP under most country's laws. Perhaps you mean patent-able inventions? 3) In the age of the Trans-Pacific Partnership, a lot of people are going to read any mention of IP in your document as an excuse for further draconian "IP protection" laws that only serve large corporate and state interests.	Action 2 Action 1: Omit section.

Morgan Qualls j.morgan.qualls@gmail.com 108.227.108.71	2	**Para 31:** *Violence against women* is defined in article 1 the Declaration on the Elimination of Violence against Women (United Nations General Assembly, 1993) to mean:	While superficially true that the phrase "any act" would include online acts, the larger context of the "Declaration on the Elimination of Violence against Women" constituting paragraph 32 is not so broad as definitions of "online violence" proposed by this report. In particular, it does not make exception to the conventional definition of violence as necessarily having a physical component.	Action 2
J. Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	2, 3	**Para 39:** '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.'	"blasphemous libel" is a legal term from English Common law meaning "publication of material which exposes the Christian religion to scurrility, vilification, ridicule and contempt, and the material must have the tendency to shock and outrage the feelings of Christians". It has nothing whatsoever to do with "violence against girls and women". Additionally, "hate speech" is extremely subjective and is always defined by those in power, usually as speech they don't want to be heard. The belief that giving states more justification for repressing unpopular speech will somehow benefit women is naive, to say the least.	Action 2, 3 Note: Commentator is reminded that the definition is quoted from a source to provide an indication of all existing definition of the problem. By quoting it, the BPF does not necessarily endorse it.
Agustina Callegari agusofi@hotmail.com 200.114.146.44	2, 1	**Para 59:** Online VAWG can impact women in different ways depending on their context or identity. This can be attributed to	I find valuable for this draft the analysis made by Roberto Castro and Florinda Riquer on VAW(In Spanish http://www.scielo.br/pdf/csp/v19n1/14913.pdf). The authors identify at least three dimensions of	Action 2 Action 1: Consider incorporating this approach and/or including a

		multiple and intersecting forms discrimination that women and girls face based on these factors. For example, women can be more at risk to diverse types of abusive or violent behaviour because of their profession, age, identity or geographical location. Some of these specific contexts or 'classifications' of women are outlined in the paragraphs below	VAW. A conceptual dimension, where it is necessary to differentiate the physical violence from the emotional and from the economic one. A temporal dimension, in which episodic violence and chronic violence are distinguished. And an evaluative dimension, which makes the difference between violence measured by objective standards and the violence subjectively perceived by women and men. As the authors point out it is possible to notice cultural differences in the valuation of each fact and what society defines as violent.	recommendation for future research to investigate different dimensions of online violence/ abuse.
Ellen Blackler ellen.m.blackler@disney.com 184.75.119.52	1	**Para 61:** There is growing recognition of the particular risks that young people and children face online in many countries around the world, including an IGF BPF on the topic in 2014.[14] Some initiatives, like that of Disney's education programmes aimed at young children (under the age of 10 years) are also designed to teach children to respect everyone online and to prevent cyberbullying, for instance.[15] However, although girls and young women are often more likely to experience certain forms of online VAWG, particularly with respect of	I would suggest we expand second sentence to include a broader range of examples of education programs. I propose. "There are also many programmes that aim to prevent bullying, cyberbullying and promote digital citizenship. Examples include, the Amigos Conectados program in Latin American (http://amigosconectados.disneylatino.com/esp/); Internet Matters in the UK (http://www.internetmatters.org/); Netsmartz workshop in the US (http://www.netsmartz.org).	Action 1: Effected change in part as follows: "There is growing recognition of the particular risks that young people and children face online in many countries around the world, including an IGF BPF on the topic in 2014. There are also many programmes that aim to prevent bullying, cyberbullying and promote digital citizenship, like the Amigos Conectados programme in Latin American, Internet Matters in the UK, and Netsmartz Workshop in

		their bodily development and sexuality, most literacy programmes and research into child online protection is not gender-specific.		the USA..." (Note relevant footnotes with links to sources not provided in this Appendix but can be found in Part 1.)
Agustina Callegari agusofi@hotmail.com 200.114.146.44	1	**Para 62:** Example: Ranking girls for alleged sexual promiscuity in Sao Paulo, Brazil	Examples in Argentina: Last years, at the Personal Data Protection Center for Buenos Aires Ombudsman's Office (a local human rights organization, we have received many complaints on "porn revenge" cases on the Internet. All victims are women whose right of intimacy has been violated causing several problems in their daily lives. As an example of one of the cases: After breaking up with his boyfriend, a woman found that several naked pictures of her and a sex tape were published without consent on a Facebook group that she shared with co-workers. The photos were also distributed in two porn websites (one based in the country and another in the US). At that time, when she put her name on a search engine, the first result was about these photos. This situation causes a damage of her daily life and, as a result, she was removed from her position to another working area. She reported the situation to Facebook, Google and the websites, but she didn´t receive any answer at all. Therefore, she made a complaint at the	Action 1: Effected change in part as follows: Incorporated examples as case study with permission; incorporated first example in Part I paragraph 60.

			Personal Data Protection Center for Buenos Aires Ombudsman's Office. Even though, after many procedures the content was removed, it is still possible to access to some images from other websites that has republished the content. However, as a step forward for the woman, the images are no more related to her name damaging her reputation. Another example: In 2013, a young girl was photographed having oral sex in a disco. The photo was published by the community manager of the place on their Facebook fan page. Instantaneously, people started to share the image and putting aggressive comments about the girl. They even created a new Facebook fan page making constantly cyberbullying. Moreover, they create also a hashtag about the photo which was used on Twitter. This last social network, after the victim report an abuse, removed the tuits. However, at that time, Facebook denied to remove the content because the image did not violate their community rules (the image was taken from far and it didn´t show any naked body). Finally, Facebook closed the group. Currently, although the photo is no longer associated with the girl name, it is still shown in many websites.	
Ashell Forde ashell.forde@gmail.com	7	**Para 77:** Religious, cultural or moral norms can	… "this can [be] put women especially at risk"…	Action 7:

104.153.134.131		also be used as methods to attack and threaten women online. In some contexts, this can be put women especially at risk to physical violence, where the line between online threats and the likelihood of offline occurrence is fine. Access to justice can also be challenging when the state or law enforcement prioritises prosecution of offences against religion, culture and morality rather than online VAWG.	The bracketed portion should be removed.	Effected change in full.
Ferreira twinzam.v@gmail.com 109.51.214.75	4	**Para 77 (above)**	Not only women are attacked or threatened online due to religious, cultural or moral norms. Many times being of one specific nationality with cultural or religious differences can be dangerous to men. Not only they can be perceived as sub human, that same disdain isnt hidden from them, they can be harassed and stalked after leaving the online world with dire consequences. Such acts are many times downplayed and disregard due to the fact they are “just men”. Justice is far more harder to strive due to the image societies have from men and that is also reflected on the results of criminal cases because of those	Action 4a

			notions.	
Ashell Forde ashell.forde@gmail.com 104.153.134.131	7	**Para 79:** Bayhaya developed a campaign as part of her work as human rights activist in Pakistan. Following the launch of the campaign she, along with her female colleagues, received serious online threats and abuse. Although she closed her social media accounts, her personal data (including pictures) were stolen and used for posters that accused her for 'blasphemy' and insulting the Quran and Prophet Muhammed.	… "stolen and used for posters that accused her" [for] 'blasphemy'"… The bracketed portion should be replaced with "of".	Action 7: Effected change in full.
Ashell Forde ashell.forde@gmail.com 104.153.134.131	1	**Para 112:** In addition to a lack of awareness and low levels of digital literacy, there is also a tendency to trivialise or normalise online VAWG, particularly on social media platforms. This apparent trend, which is arguably related to a lack of awareness of the effects of online VAWG, is particularly harmful as it contributes to gender inequalities and a culture that may be increasingly hostile to female Internet users. An example includes the sharing of pictures of injured women with captions	Another useful example may be the website reddit.com where there exists a subreddit called Cute Female Corpses. Users post graphic photos of dead women, sometimes with their genitals exposed while other users comment on the sexual attractiveness of the corpse.	Action 1: Example not incorporated due to perceived lack of direct relevance.

		like 'next time don't get pregnant' on Facebook.		
Lasershark mlwtxapj@sharklasers.com 95.33.110.216 (linked to J)	1	**Para 115:** For victims, a lack of support frequently extends to the legal and political environments they find themselves in. Authorities, including police officers, are sometimes unsympathetic, tend to lack relevant training in how to address online VAWG, and often do not have the necessary equipment for finding evidence of online VAWG…	**[often do not have the necessary equipment for finding evidence of online VAWG]** What would that equipment be? Wouldn't a computer with Internet access be enough to view and save the evidence or are you talking about giving the police some sort of global Facebook read permissions for example, or Internet monitoring/logging equipment installed in major Internet nodes?	Action 1: Clarified sentence to prevent potential misunderstanding: "Authorities, including police officers, are sometimes unsympathetic, tend to lack relevant training in how to address online VAWG, and sometimes do not even have the necessary equipment (e.g. computers with Internet access) and/or technological skills or awareness for finding evidence of online VAWG."
Agustina Callegari agusofi@hotmail.com 200.114.146.44	1	**Para 130:** Lastly, the cross-jurisdictional nature of the internet means that authorities, including law enforcement or even internet intermediaries like telecommunication companies can find it difficult to investigate and pursue cases of online VAW.	The difficult to investigate across countries, it is one of the main problems to address online VAW. The way that the information circulates on the Internet makes extremely difficult for a national agency to, for example, stop the damage that a naked photo of a woman publishes without consent could make. As it is highlighted in this report, the cooperation among all stakeholders in a local and in an international level is fundamental in order to address this issue.	Action 1: Updated Part II paragraph 60: "Lastly, the cross-jurisdictional nature of the internet means that authorities, including law enforcement or even Internet intermediaries like telecommunication companies can find it difficult to investigate

				and pursue cases of online VAW; reinforcing the importance of cooperation amongst national and international stakeholders." Also included example from one of Agustina's submitted examples in section on jurisdiction.
Lasershark mlwtxapj@sharklasers.com 95.33.110.216	8	**Para 137:** Women who are prominent and find themselves in public spaces tend to face more abuse (see paragraphs 98 to 106 above). Women also often face threats and violence after political articulation or participation, and, similarly, women who are famous (e.g. actors) also tend to experience more online violence or abuse than women who are not as well-known.	Isn't that self-evident? If 1% of the people you interact with online are harassers the total number of harassers will go up the more well-known you are. I don't see how this is anything beyond simple math.	Action 8
Lasershark mlwtxapj@sharklasers.com 95.33.110.216	3	**Para 149:** Tensions around competing rights have often been raised in discussions to address online VAWG; particularly through measures that involve the takedown of content, which brings to question issues of freedom of expression.	This is not only a somewhat obscured call for the end of anonymity online but also completely misses the fact that women can be, and profit from, anonymity as well. After all, if nobody knows who you are, what you look like, what gender you identify as, the only thing they have to go on is what you write. You can even pick a pseudonym and drop whenever you want to. This is a powerful tool for	Action 3 Note: As the commentator can read in the report, the importance of anonymity to protect free speech and enable people to participate online is

		Women's rights advocates have responded by stating that online VAWG in effect curtails women's right to freedom of expression by creating a hostile and unsafe online environment that can result in women withdrawing from online spaces. Similarly, while anonymity and the protection of privacy are often described as vital for the exercise of freedom of expression online, these rights also enable online VAWG by hiding the identities of perpetrators (as explained in paragraphs 90-93 above). There is thus a need for measures that protect women online to consider, include and balance multiple rights including the right to safety, mobility, to participate in public life, freedom of expression, and privacy; and to take into account existing inequalities and discrimination which may affect how rights are protected and recognised. Such balancing exercises need to consider the importance, nature and extent of any limitation proposed and should opt for the less restrictive means to achieve the purpose.	women and men alike and should not be curtailed. Not to mention, if you build up the kind of infrastructure that can end online anonymity you are also playing into the hands of oppressive regimes that want to censor and punish their citizens. Just look at China for example, a country where you can be detained and murdered for running a blog.	also acknowledged by the BPF, alongside the importance of protecting women's rights. Sometimes these anonymity and women's rights need to be balanced, however.
J Carl Henderson j.carl.henderson@gmail.c	1	**Para 161:** In the state of **California** (USA), the	The Electronic Frontier Foundation (EFF) opposed the CA law. (https://www.eff.org/mention/post-	Action 1: Incorporated section on Arizona

om 72.64.98.120		controversial SB 255 Electronic Communication Devices: Prohibited Distribution of Personal Information Act[55] came into effect in October 2013 and creates a new misdemeanour of disorderly conduct by way of distribution of intimate photographs with the intent to cause serious emotional distress. The Act is narrowly worded and focuses on instances in which the person who takes or makes the intimate image, distributes it with the intent to cause, and the effect of causing, serious emotional distress to a victim.	revenge-porn-california-and-you-may-go-jail) and the ACLU fought and won a victory in US federal court against a similar law in Arizona (https://www.aclu.org/blog/speak-freely/victory-federal-judge-deep-sixes-arizonas-ridiculously-overbroad-nude-photo-law)	law as follows: "In Arizona, the Arizona Revised Statute 13-1425 was passed in 2014 with the objective of preventing revenge pornography, but with far broader implications. In a recent case, *Antigone Books v. Brnovich,* the plaintiffs argued that the law amounted to the unconstitutional limitation of free speech by criminalising more than only offensive actions. In accordance with the court order, prosecutors in the state were ordered to halt the enforcement of the law." (Note relevant footnotes with links to sources not provided in this Appendix but can be found in Part 1.)
J lcxbyyee@sharklasers.com 68.181.252.5	1	**Para 161 (above)**	I'm unclear on what you'd rather California have. Should we have a policy that *any* distribution of "intimate" photographs is a misdemeanor/crime? So someone who posts amateur pornography with the knowledge and consent of his/her partner is guilty?	Action 1: To make it even clearer that the California position is not necessarily supported, added the following clause: "It has been criticised for

				potentially criminalising speech and allowing prosecution in victimless instances."
J lcxbyyee@sharklasers.com 68.181.252.5	2, 1	**Para 163:** There is a need for public sector initiatives to acknowledge and recognise that although online VAWG might not cause actual physical harm in all instances, it can also cause significant **emotional and psychological harm**, as well as impact on issues such as mobility, employment and public participation (see Section B above for a thorough exploration of consequences). These are equally important factors to address and prevent.	What constitutes "significant emotional and psychological harm" is deeply subjective and ambiguous. There's no objective brightline of any kind. If one isn't provided, then this has the makings of a Salem Witch Trials style horrorshow where a woman (because of *the way that this entire document is worded*, **not** because she's a woman) could accuse a man of inflicting significant emotional and psychological harm and we'd have no real way to evaluate her claim because it's subjective. This does not make for any sort of feasible law.	Action 2 Action 1: No action taken. Note: When emotional and psychological harm is concerned, it is difficult if not impossible to have any objective measurement. Also, the section does not ask for 'any law'.
Ellen Blackler ellen.m.blackler@disney.com 184.75.119.52	1	**Para 168:** **Challenges and lessons learned** (heading)	I think these should be characterized as "challenges and ideas for further exploration," as they are not consensus proposals or conclusions.	Action 1: Recommended change effected.
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	1	**Para 177:** The **Broadband Commission** for Sustainable Development, an initiative steered by UNESCO and the ITU, was established in May 2010…	That report has been withdrawn for numerous errors. There is no way to know if the revised report will contain the content you are citing.	Action 5

Ashell Forde ashell.forde@gmail.com 104.153.134.131	7	**Para 182:** **Twitter**'s abusive behavior policy is aimed evaluating and addressing potentially abusive behaviour on the platform if it is in violation of the Twitter Rules and Terms of Service…	…"Twitter's abusive behavior policy is aimed [at] evaluating and addressing potentially abusive behaviour"… The bracketed portion should be included.	Action 7: Recommended change effected in full.
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	1	**Para 182 (above)**	Twitters abusive behavior policy is also very subjective, and prone to being gamed. Mass abuse reports by a small organized group can cause Twitter to suspend accounts that don't violate their rules.	Action 1: Example included as part of paragraph 72: "It was also noted by another commentator that Twitter's abuse policy tends to be subjective and subject to abuse by users. The submission of a significant number of abuse reports by a small group of organized people may, for example, lead to the suspension of accounts without a clear violation being present."
J Carl Henderson j.carl.henderson@gmail.com	1	**Para 184:** Twitter enables users to report violations and welcomes complaints or reports from	Twitter has no "privacy laws" They are a corporation, lacking the legal capacity to make laws. This should say "Twitter has also changes its	Action 1: Change effected as follows:

72.64.98.120		both individuals that experience abuse and third party complaints. Twitter has also changed its privacy laws from making tweets available for only 30 days to making all tweets since Twitter was created available and searchable on their website; which is helpful in collecting evidence in past cases of online harassment.	privacy rules…"	'laws' changed to 'rules'.
Agustina Callegari agusofi@hotmail.com 200.114.146.44	1	**Comment on paragraph 186:** *Challenges and lessons learnt:*	Generally speaking, the lack of statistics on violence against is pointed out as one of the main problems to address this issue both online and offline. It is important to start thinking about how to promote the compile of these numbers.	Action 1: Importance of more research and statistics to measure incidence of online violence/ abuse stressed in text (Part I paragraph 104) and in recommendations. Potentially include quote from commentator stressing importance of statistics in Part I.
Morgan Qualls j.morgan.qualls@gmail.com 108.227.108.71	2, 1	**Para 195:** These initiatives have diverse objectives, including raising awareness about how to support victims; promoting digital safety education; enabling crowd-sourced blocking; identifying ('naming and shaming') perpetrators; encouraging	It should be noted that "crowd-sourced blocking". "identifying ('naming and shaming') perpetrators", and "norm-setting on online behaviour" are activities that meet the definition of online violence as promulgated in this report.	Action 2 Action 1: Clarified that under specific circumstances, certain online actions may either be used to protect or abuse or violate

		public debates to promote norm-setting on online behaviour; and direct interventions in response to active (or real) cases of online VAWG. While it is impossible to highlight and describe each of these here, a few examples of these initiatives include…		someone's rights.
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	7	**Para 207:** Footnotes	You have a lot of URLs that are not rendering as links. I'm going to stop noting each one, and just leave a general reminder to check this in your next draft.	Action 7
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	7	**Para 207 (above):** Footnotes	A general note on your citations. You really should include more information, so people can read the relevant parts for themselves—and to reduce their vulnerability to "link rot" over time. I'd recommend for clarity that citations include the following: Title URL Publisher/Institution (spell out acronyms) Authors Date Page Number(s)	Action 7 Note not all these details are available, but are included as far as is reasonably possible.

J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	3	**Para 213:** *Broadband Commission, Cyber Violence against Women and Girls: A world-wide wake-up call (2015). Available online: http://www.broadbandcommission.org/Documents/reports/bb-wg-gender-report2015.pdf.*	You've cited the "*Broadband Commission, Cyber Violence against Women and Girls: A world-wide wake-up call (2015)"* report. Please note that the Broadband Commission withdrew that report and any links to it currently go to a page saying "This report is currently in revision and will be re-posted as soon as all relevant inputs have been taken onboard."	Action 3
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	7	**Para 219:** *This list was identified by BPF participants as people who might be particularly vulnerable to online VAWG and is not an exhaustive list.*	Without more context (or at least expansion of the BPF acronym) this citation (and the next) are kind of unclear.	Action 7. Note: The acronym was defined in the introduction.
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	7	**Para 222:** *Example submitted by Ellen Blackler, The Walt Disney Company, USA.*	Unless this note appears on the same page as the text it is commenting on, I would suggest more context	Action 7. Note: In Draft IV, footnotes appear on same page.
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	7	**Para 228:** *See:* http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/181	Bare URLs as references can cause problems when documents move or vanish. It's really best to include, title, author, date, publisher/institution info, too.	Action 7
J Carl Henderson j.carl.henderson@gmail.com	7, 1	**Para 228 (above)**	Unless this note appears on the same page as the text it is commenting on, I would suggest more context. (This comment is duplicated because it	Action 7. Note: In Draft F, footnotes

72.64.98.120			applies to two or more citations.)	appear on same page.
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	7, 1	**Para 231:** *See @sonaliranade.*	Are you citing a specific tweet or all the tweets ever by this person? The current reference does not identify any specific tweet or tweets, but instead her entire twitter stream. URL does not render as a link.	Action 1: Deleted footnote reference to Twitter account, which was for illustrative purposes. Action 7. Note: In Draft F, footnotes appear on same page.
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	7	**Para 235:** *A Dutch study, for instance, showed that lesbians were 6.4% more likely to experience online bullying than heterosexual women. See European Union Agency for Fundamental Rights (FRA) (September 2014). Violence against women: European Union survey results in the Dutch context. Available online: goo.gl/L66swK.*	Use the URL to the full report instead: http://www.atria.nl/atria/mmbase/attachments/347430/Violence_against_women.PDF	Action 7 Action 1: Change effected in full.
J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	7, 1	**Para 261:** *Note that the term 'tort' generally refers to a crime perpetrated by an individual.*	This is incorrect. Torts are not crimes; rather they are "civil wrong which can be redressed by awarding damages". (https://www.law.cornell.edu/wex/tort)	Action 7 Action 1: Removed definition as it depends on jurisdiction.

J Carl Henderson j.carl.henderson@gmail.com 72.64.98.120	7	**Para 262:** *Available online: https://legiscan.com/CA/text/SB255/id/863412/California-2013-SB255-Amended.html.*	You are linking an an earlier version of the CA bill; not the one that was passed and signed into law. Try (https://legiscan.com/CA/text/SB255/2013).	Action 7 Action 1: Change effected in full.

Comments on Draft II received over email:

Ellen Blackler (submitted over email on 21 October 2015) Ellen.M.Blackler@disney.com	1	**Para 166:** Some countries also tend… An example is the UK government's adoption of filters to address the distribution and viewing of online child abuse images. While probably well-intentioned, these filters were designed in a way to over-filter content (including sex education websites) and users struggle to find information regarding why certain sites are inaccessible.[56]	I think the statement footnoted by footnote 56 is not accurate and not a fair conclusion based the thoughtful discussion in the footnoted Freedom House report. I would suggest the two sentences preceding footnote 56 be deleted and replaced with a footnote that reads something like: "For an interesting discussion on the challenges and efficacies of efforts in the U.K. to address the distribution and viewing of child abuse images online, see [the Freedom House report]."	Action 1: Change effected in part as follows – see para 105: "…although such measures need to be transparent at all times. For an interesting discussion on the challenges and efficacies of efforts in the UK to address the distribution and viewing of child abuse images online, including the tendency of such filters to also block legitimate online content, see Freedom House's *Freedom on the Net* (UK edition) report]. (Note relevant footnotes with links to sources not provided in this Appendix but can be found in Part 1.)

Patricia Cartes (submitted over email on 20 October 2015) Patricia@twitter.com	1	**Para 182 (section on Twitter)**	In March Twitter introduced a change that makes it easier for users to report threats that they felt may warrant attention from law enforcement. This change was the result of direct feedback from safety partners specializing on VAWG like NNEDV. After filing a report regarding a threatening Tweet directed at users, they'll see an option on the last screen to receive a summary of their report via email. Clicking the "Email report" button sends the user an email that packages the threatening Tweet and URL along with the responsible Twitter username and URL and a timestamp as well as the reporter's account information and the timestamp of their report. Twitter's guidelines for law enforcement are also included as they explain what additional information the company has and how authorities can request it. Structures of Single Points of Contact (SPOCs) in the Law Enforcement world, which have been implemented in countries like the UK,	Action 1: Inserted summarised version of contribution– see paragraph 119: "In March 2015, Twitter also introduced a change that makes it easier for users to report threats that they felt may warrant attention from law enforcement. When filing a report regarding a threatening tweet, the complainant has the option to receive a summary of their report via email. Clicking the "Email report" button sends the complainant an email that packages the threatening tweet and URL, responsible Twitter username and URL, a timestamp, as well as the complainant's account information and the timestamp of the report. Twitter's guidelines for law enforcement are also included in the report, including an explanation of what additional information Twitter has and how authorities are able to request it. In addition, structures of single points of contact (SPOCs) in law enforcement, which

			make it easier for members of the public and internet companies to react to this type of content.	have been implemented in countries like the UK, may make it easier for members of the public and Internet companies to react to online abuse and violence."

d) Part III: Appendices (11 comments)

Name/ email/ IP/ date	Code	Section/ para/ heading concerned	Comment (verbatim)	Action/ notes
Ferreira twinzam.v@gmail.com 109.51.214.75	6	**Para 17:** A total number of 56 responses were collected, with the largest proportion of responses submitted by respondents who identified themselves as part of the civil society stakeholder group (41%), and the smallest number from the technical community (4%). It should be noted, however, that the identified stakeholder groups were not necessarily mutually	56 responses is a very small number to conduct a survey. even by high school standarts Considering the countries picked (for example from Europe) the data is so limited that those countries aren't enough to represent the continents they are from.	Action 6

		exclusive. Of these stakeholders, 31 respondents also identified their organizations, which varied from civil society organizations to police and government departments, universities, intergovernmental organizations, etc.		
V.Z streptococcus.viridans@gmail.com 80.220.78.108	6	**Para 17 (above)**	56 responses is an extremely small sample size, even more so considering the respondents come from a variety of continents.	Action 6
Johnny Numeric johnnynumeric@gmail.com 65.80.202.133	8	**Para 36:** "cyber bullying" and/or repeated harassment through unwanted messages, attention and/or contact	#takebackethetech internet should be uncensored people need yo grow up learn to take a joke and stop crying all the time	Action 8
Erika Smith erika@apcwomen.org 201.145.222.99	1	**Para 40:** hacking websites, social media and/or email accounts of organisations and communities	One question is if we want to use the term "hacking" in a negative way. In Mexico and many countries the term hacker and hacking are trying to be re-conceptualised – taking back of the term – as people who open up spaces, code etc. for communal	Action 1: Changed references to hacking to 'cracking', and include a footnote to explain the reasoning behind the change: "The term 'cracking' is used rather

			good/learning. CRACKING on the other hand is seen in a different light. I think "cracking" as a term is less well known, we could use it and footnote, or we could say forced entry/takeover?	than 'hacking' to indicate a forced entry or takeover of content with malicious intent, while 'hacking' could include similar actions that are bona fide and/or done in the public interest."
Johnny Numeric johnnynumeric@gmail.com 65.80.202.133	8	**Para 40 (above)**	Video – S4T	Action 8
Johnny Numeric johnnynumeric@gmail.com 65.80.202.133	8	**Para 52:** The UN Broadband Commission for Digital Development Working Group on Broadband and Gender report on "Cyber violence against women and girls" defines cyber violence against women and girls to include…	Why is it you openly invite constructive dialouge, yet when approached with valid criticism you refuse to debate, and yell "harassment"? Your agenda has been exposed. TRIPLE WEASEL WHOPPER	Action 8
Johnny Numeric johnnynumeric@gmail.com 65.80.202.133	8	**Para 52 (above)**	#takebackethetech	Action 8
Johnny Numeric johnnynumeric@gmail.com	8	**Para 52 (above)**	#takebackethetech internet should be uncensored people need yo grow up learn to	Action 8

65.80.202.133			take a joke and stop crying all the time	
Chester k.whitey@aol.com 50.179.93.215	3, 8	**Para 52 (above)**	You're using the old report, which had blank citations, as a citation for this report. You say that abusive comments, and verbal online abuse are equal to violence. Then you welcome constructive dialogue for your report, and yell harassment when you're criticized.	Action 3; 8
Ferreira twinzam.v@gmail.com 109.51.214.75	4	**Para 55:** Various respondents stressed that online violence not only permeates the offline sphere, but also often extends from offline environments (and patterns of abuse, like ongoing domestic abuse) into an online sphere (i.e. vice versa). Online VAW thus needs to be studied whilst keeping the offline environments in mind.	Online violence doesn't exist. At best you have cyber bullying. There isn't even a distinction of verbal and physical abuse. The way these points are made put verbal and physical abuse in the same category.	Action 4b

Evelyn Namara	n/a	COMMENTS ON SURVEY QUESTIONS		n/a Note: comments relate to survey – and are an attempt to respond to survey questions. As the survey analysis is finalised, no further submissions can be received.

APPENDIX 5: SOCIAL MEDIA CAMPAIGN

Background

As a part of the BPF's objective of engaging as many stakeholders as possible on the issue of online abuse and gender-based violence against women, BPF participants decided to gather further stakeholder input on one of the BPF's sections of work, namely the impact of online abuse and gender-based violence. The social media platform Twitter was used for this purpose.

Participants were asked to sign up to a "headtalker" campaign[145] that allowed an automatic tweet to be sent from the Twitter accounts of people who had signed up. The tweet concerned was:

> "What impact does online violence have on women and girls? Use #takebackthetech to contribute examples to #IGF2015"

In addition to the hashtag #IGF2015, the BPF decided to use #takebackthetech for the conversation due to the latter hashtag's familiarity and recognisability among many in the technical community that the BPF wanted to gather input from. #takebackthetech is frequently used by the Association for Progressive Communications (APC), which since 2006 has used the related Take back the Tech! campaign[146] to address and combat online violence and abuse.

BPF participants were requested to share details of the campaign with their communities with the aim of gathering input from diverse countries and stakeholder groups, and were encouraged to translate the tweet into their region's language.

Context

At the time of the scheduled Twitter conversation, the BPF's second draft document (Draft II) had been published on the IGF's review platform with the aim of gathering stakeholder input on the BPF's written work. The social media campaign was planned with the aim of also encouraging stakeholders to comment on the draft and to, as far as possible, gather input that could potentially be used to further augment a pre-existing theme of the BPF's work, namely impact, with primary examples.

Shortly before the BPF's Draft II was published and before this social media campaign was planned, the UN Broadband Commission published a report on a similar topic than the BPF's work, namely cyberviolence against women and girls.[147] The report attracted

[145] Available online: https://headtalker.com/campaigns/share-our-tweet-on-08-October/. [Accessed 28 November 2015].
[146] Take Back The Tech! (website). Available online: https://www.takebackthetech.net/know-more. [Accessed 28 November 2015].
[147] Broadband Commission (September 2015). *Cyber Violence against Women and Girls: A world-wide wake-up call.* Note that at time of publication of Draft F, the report had been withdrawn with the aim to update

a lot of publicity and later criticism and was subsequently withdrawn for further input and updating, although it remained available online.

Counter campaign/ attempted attack of BPF's efforts

The day before the social media campaign was scheduled to commence, 9 October 2015, BPF participants started receiving tweets and emails warning and threatening them of an effort to hijack and derail the BPF's planned social media campaign (henceforth 'the attack'). One email to a participant, for instance, included the following threats (*sic*) (note that while the identity and contact details of the sender is known to BPF participants, it is not disclosed for legal reasons):

> *"I hope you enjoyed how your whole campaign got destroyed preemptively. I've been waiting to strike and today was a glorious day. Tomorrow will be better. Your whole operation to shut down free speech online has been exposed, and you haven't even felt the wrath of the mainstream media yet. Just wait. The stories are starting to break. Your hashtag is already destroyed, most likely permanently. All of your groups information has been downloaded and archived. Scrubbing it now won't do any good, and will actually make things worse..."*

The attack took place on platforms like Twitter, Facebook, email, blogs, some small online publications, and the IGF's review platform, where Draft II of the BPF's outcome document was published (see Appendix 4). It included messages, images, memes, 'opinion' pieces and videos.

In the course of two days (one weekend), over 25,000 tweets and retweets were gathered on the hashtag #takebackthetech, and some BPF participants received direct tweets, often threatening and misogynistic in nature. 15,225 tweets included links (pictures or weblinks), while 835 tweets were replies (indicating actual attempts at a conversation rather than just filling the hashtag). The APC's Wikipedia page was altered (although quickly restored), and there was also a possibly related brute force attempt to gain access to the IGF's review platform where the BPF's Draft II had been published. Some BPF participants were furthermore contacted by individuals purporting to be from media outlets in the hope of eliciting personal information about other BPF participants. These attempts were easily identifiable as false and failed.

At more or less the same time, BPF participants found content on platforms like Reddit[148] and 8chan that indicated the concerted nature of the attack on the BPF's campaign. One comment, for example, read:

> *"Who's down to raid tonight? Last time we had 20, and I'd like to get a group of 100. So tag any friends who might be interested in raiding in the comments."*

---

and fix mistakes. As at 26 November 2015, the report remained available online at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259. [Accessed 29 October 2015].

[148] For an example, see this archived message thread, available online: https://archive.is/aRi5J#selection-9621.0-9657.7. [Accessed 27 November 2015].

Many of the individuals involved in the attack seemed to associate themselves with the so-called Gamergate community (whilst remaining mostly anonymous and/ or using pseudonyms). An email received by one of the BPF's participants, for instance, contained the following claims (note that while the identity and contact details of the sender is known to BPF participants, it is not disclosed for legal reasons):

> *"Behold, I am the leader of GamerGate and you are only beginning to feel the wrath of legitimate political activism in this new era…. But darling, you are just beginning to feel what it's like to get dunked on. We will not stop at destroying your campaign and jamming it up so that you can't even function publicly…"*

Much of the content of the tweets and other messages seemed to derive from misunderstandings, including a confusion of the BPF's work with the UN Broadband Commission report; a misunderstanding of UN structures and the IGF's work; a related misunderstanding of the methodologies of BPFs and the IGF as open, transparent, community-driven, and multistakeholder platforms; and the misinformed belief that the BPF's work was somehow aimed at limiting free speech online under the guise of protecting women. With little exception, most content suffered from a severe lack of misunderstanding of UN and IGF processes, the roles of BPF coordinators and contributors, as well as the 'status' of the BPF's intended outcome.

In addition, much of the content appeared to be aimed at intimidating, silencing and exposing private information about BPF participants; contained misogynistic and sexist language and imagery; contained racist and xenophobic messaging; was homophobic and/ or transphobic in nature; and many tweets contained graphic images and content of sexualised violence.

Common messages included:

- Online violence against women is not real violence
- Violence happens against men too
- Feminism is about censoring men
- Gender studies is worthless
- Women just choose not to study STEM
- Women are too weak if they cannot handle criticism
- Women should not be in technology fields
- Women should shut up/ be silenced
- #takebackthetech hurts women in tech by making them victims
- #takebackthetech is a bunch of white, privileged feminists
- #takebackthetech uses women in "developing" countries
- #takebackthetech minimises "real" violence
- The BPF is run by the UN
- The BPF report is another version of the Broadband's Commission's report
- APC is part of the UN and wants to censor everyone
- APC is a bunch of professional victims
- APC has loads of money from questionable sources

Some of the actors involved in the attack also attended open and freely accessible BPF virtual meetings using false names and impersonating other (real) people. These kinds

of actors, of whom there were fortunately few, seemingly aimed to compromise the open and participatory format of the IGF's BPFs and derive from a clear and unfortunate misunderstanding of the ways in which to participate in the IGF's multistakeholder work.

The positive responses that were collected in response to the BPF's campaign and that did not form part of the attack were summarised by the APC on Storify.[149]

How did the BPF respond to the attack?

The primary strategy adopted by the BPF in addressing the attack was one of limited engagement whilst continuing the BPF's work as usual. The BPF notified all BPF participants who appeared in or were identified in media (like videos) to enable them to take the necessary steps to protect their privacy. Emails notifying people of the attack were also sent to the IGF's multistakeholder advisory group (MAG) and the BPF's mailing list; reminding participants of the IGF's code of conduct.

In a blog post issued in response to the attack, the chair of the MAG, Ambassador of Latvia Jānis Kārkliņš, noted:[150]

> *"I also wanted to reflect here on a recent event that highlights the importance to continue building on the IGF's commitment to principles of openness, transparency and respect. Last week the Twitter conversation convened by the BPF on Countering Online Abuse and Violence Against Women was unfortunately the target of an online harassment campaign… While it was truly regrettable that a small group of individuals decided to engage in this type of behavior, it reinforces at the same time the need for such best practices. Today, it has strengthened the group's resolve and determination to continue their excellent work on this important topic… The value of IGF outputs is indeed intimately linked to the open, bottom-up and transparent nature of the process. Discussions on the various topics are healthy, but need to be led in a constructive manner. The BPF leaders have learned from this experience and are continuing the work leading into the upcoming IGF in Brazil from 10-13 November."*

No participants or attackers were expelled or blocked from any IGF platform – including meetings, the review platform and the mailing list. Only one of the 96 comments received on the BPF's Draft II was not accepted due to the use of obscene and racist language that did not meet the IGF's code of conduct (see Appendix 4). Whilst BPF participants were generally aware of the identities of attackers who were attending virtual meetings, they nevertheless welcomed them and continued their work as usual.

The BPF also adopted extra measures to increase transparency in dealing with comments and input from the community on its draft documents. Each comment on

[149] Storify (n.d.) *Take Back the Tech – 9 October 2015.* Available online: https://storify.com/APC_News/takebackthetech-9-october. [Accessed 27 November 2015].
[150] IGF (16 October 2015), *IGF takes action, developing best practices to address Internet issues*. Available online: http://www.intgovforum.org/cms/magabout/mag-chair-s-blog. [Accessed 30 November 2015].

Draft II, for instance (many of which were easily identifiable as being part of the attack), were analysed individually using a thematic approach and the actions taken to address each comment (including how and where the report was updated) are listed in Appendix 4.

Strategies adopted by APC

APC, who were directly involved and affected by the attack because of the use of #takebackthetech, at first also adopted a non-engagement strategy. After a few days, some APC staff members started engaging tactically and more directly with a few of the attackers tweeting under #gamergate and #takebackthetech, particularly those asking questions that involved criticising APC's work and questioning the existence of online abuse and violence. Staff members did this with the knowledge of APC and using their personal Twitter handles.

APC released two statements to denounce the situation, to provide information on the attack and its basis, and to call for support from the community. The first one was published on 10 October 2015,[151] the day after the attack began, offering a response, informing the APC community of the situation, and sharing strategies for supporting APC and the BPF. The second statement was published on 12 October 2015 with facts about the Take Back the Tech! campaign and clarifying the false arguments that were being circulated as part of the attackers' strategy.[152] In one week the statements received a high number of reads (2080 reads on the first, and 3264 reads on the second statement). These statements were shared with media outlets, individual journalists, partners, members and engaged activists, and were republished and shared among other networks.

Various efforts to improve and strengthen the security, privacy and safety of online spaces and interaction of APC members and the Take Back The Tech campaigners were also made during this time (although they will not be disclosed here in the interests of continued safety and security. APC notified contacts at Twitter about the situation, but did not request for specific action. At the same time, individual users reported some of the most violent and misogynistic tweets that they received.

Part of the APC team took the lead on the evidence-building process of gathering all tweets, images, messages, emails, forum planning comments, etc., that were produced as a part of the attack.

Some consequences of the attack

As a result of the attack, some participants disengaged from the IGF's open and inclusive, transparent platforms because they felt unsafe and had concerns related to

[151] APC (10 October 2015), *Take Action for #TakeBackTheTech and #Imagineafeministinternet*. Available online: https://www.apc.org/en/pubs/take-action-takebackthetech-and-imagineafeministin. [Accessed 30 November 2015].
[152] APC (12 October 2015), *Facts on #TakeBackTheTech.* Available online: https://www.apc.org/en/pubs/facts-takebackthetech. [Accessed 30 November 2015].

their privacy being infringed. For example, actors associated with the attack indicated a proclivity to using video and audio material out of context with the aim of distorting the actual purpose and context of the participants' work. The attack therefore had the unfortunate effect of chilling free speech and silencing and intimidating individuals who were previously actively involved in the BPF's work.

The attack was also time-consuming as a result of the need for taking extra measures to protect participants in the future, including by having to implement emergency moderation measures. As far as possible, however, the BPF continued its work as usual and remained committed to IGF values of transparency and inclusivity, with the overarching aim of engaging as many stakeholders as possible.

The attack also exposed the BPF to one particularly difficult challenge in multistakeholder policymaking, namely when certain actors choose not to engage using existing and designated channels but flood the process in a negative campaign-like manner with the aim of derailing the process; despite the existence of other ways for them to interact reasonably, constructively and in bona fide manner.

On a positive note, the attack alerted more individuals and organizations to the importance of addressing the challenge of online abuse and gender-based violence. It led to substantial support from a multitude of individuals and organizations and raised awareness of the importance of addressing the challenge. It also provided the BPF with substantially more input and data with which to improve its work – as is discussed in the section below.