Cyberviolence Against Women and Girls in the Commonwealth

The Commonwealth

Cyberviolence Against Women and Girls in the Commonwealth

The Commonwealth

UK International Development

Partnership | Progress | Prosperity

Published by the Commonwealth Secretariat.

Contents

Executive Summary 1

1. Background 2

2. Nature of the Problem of Cyberviolence 3

Defining cyberviolence against women and girls 3

Types and modes of cyberviolence 4

Intimate partner and dating violence 7

Incidence of cyberviolence 7

Impact of cyberviolence 8

Bystanders 9

Challenges in responding effectively 9

3. Responses to Online Violence 10

Legal responses 10

Programme responses 12

The role of ICT companies/platforms 13

4. Conclusions 15

Executive Summary

This report provides a summary of the findings and recommendations contained in the five regional reports *Addressing the Role of Bystanders on Online Violence Against Women and Girls in the Commonwealth* produced by the Secretariat in 2023. The report presents the root causes and impacts of cyberviolence as being gender based, with a disproportionate impact on females where there is intersectionality of race, ethnicity, religion, sexual orientation, poverty, disability and other socio-economic factors.

The report notes that there are similarities between types of violence against women and girls that occurred in offline and online spheres, with some of these crimes originating in one sphere and concluding in the other. Notable types of online violence against women and girls (OVAWG) include doxing, cyber-harassment, sextortion, cyberstalking and non-consensual distribution of intimate images. The report also notes that various regions of the Commonwealth have reported a high incidence of cyberviolence, especially against women and girls.

The report highlights the role of the bystanders and their criminality or civil liability which, arguably, are relatively new considerations in the OVAWG space and makes various recommendations for Commonwealth law ministers to consider.

Finally, the report proffers a Commonwealth Action Plan as an illustrative guide for various activities and programmes that could be implemented by relevant stakeholders to combat OVAWG effectively across the Commonwealth.

1. Background

Cyberviolence is emerging as one of the largest threats facing the online world today, especially since the COVID-19 pandemic. Recent surveys conducted across countries worldwide have indicated that women and girls are victimised disproportionately online as compared with men and boys. Within the Commonwealth, cyberviolence is recognised as a serious problem, notably as it affects the full realisation of gender equality and violates women's rights.

With a grant under the UK Foreign, Commonwealth & Development Office (FCDO) Conflict, Stability and Security Fund (CSSF) Programme, in 2023 the Commonwealth Secretariat produced five regional reports on *Addressing the Role of Bystanders on Online Violence Against Women and Girls in the Commonwealth*.[1] These groundbreaking reports investigated the impact of online violence against women and girls (OVAWG) and the extent to which existing laws in Commonwealth countries hold perpetrators and others culpable for these acts.

In line with the objectives set out in the 2018 Commonwealth Cyber Declaration and reiterating the recommendations made at the 2014 Commonwealth Law Ministers Ministerial Meeting (CLMM) in Botswana, the regional reports recommended that a holistic and integrated approach be adopted to address issues of violence against women.

This report[2] is a synthesis of the major findings and recommendations of the five regional reports. It also includes a Road Map (Action Plan) as a way forward to address the problem of online violence against women and girls. The Action was endorsed by the Commonwealth Law Ministers at their 2024 Meeting held in Tanzania.

1 Africa: https://www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/book/1099; Asia: https://www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/book/1097; Caribbean and the Americas: https://www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/book/1091; Europe: https://www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/book/1103; Pacific: https://www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/book/1093;(hereinafter referred to as the *Africa Report*, the *Asia Report* etc., respectively).

2 Authored by Donald K Piragoff, KC, retired, formerly Senior Assistant Deputy Minister (Policy), Department of Justice, Canada.

2. Nature of the Problem of Cyberviolence

Defining cyberviolence against women and girls

In essence, there are two components to the definition of cyberviolence against women and girls. The first is the concept of 'violence against women and girls', and the second is that such violence is committed by means of, or facilitated by, information and communication technologies (ICTs). In regard to the first component, a number of international instruments define violence against women and girls. For example:

Article 3 of the Istanbul Convention 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.*[3]

The Declaration on the Elimination of Violence Against Women, adopted by the United Nations General Assembly, defines violence against women as:

> *Any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.*[4]

Common to these definitions is that the violence, or threat thereof, is gender based and includes all forms of harm, including physical, psychological, sexual, social and economic.

Regarding the second component involving the use of ICTs, acts of violence committed by means of, or facilitated by, information and communication technologies has been defined by the Council of Europe as:

> *Cyberviolence is the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.*[5]

While the Council of Europe definition is gender neutral, cyberviolence that is gender based, and which is specifically directed at women and girls, is of particular gravity and social concern. The regional reports noted that while both men and women experience violence through social media, women and girls are at greater risk than men and boys of experiencing cyberviolence, especially severe types of harassment and sexualised online abuse. Such acts are often rooted in larger social and cultural problems, including sexism, rape culture and misogyny, which is similar to violence in the offline world. Women and girls often find themselves in a continuum of violence both offline and online in which they feel isolated, humiliated and emotionally distressed. However, online violence has some particular troubling differences: victims can be accessible at any hour of the day, even in the safety of their own homes; perpetrators can be shielded by anonymity and geographic distance, which may increase any disinhibition to act and provoke a greater degree of anonymous cruelty; and the use of technology provides ease of access to the victim/survivor, and any content posted may become a part of the victim/survivor's permanent online identity.

3 Council of Europe Convention on Violence against Women and Domestic Violence (CETS 210), ('the Istanbul Convention'), https://rm.coe.int/168008482e

4 UN Women, 'Violence against women', http://www.un.org/womenwatch/daw/vaw/v-overview.htm

5 Council of Europe/ Cybercrime Convention Committee, T-CY (2017)10 [EN] Mapping study on cyberviolence, July 2018 | [FR] Etude cartographique sur la cyberviolence, juillet 2018, p. 5, www.coe.int/cybercrime, [hereinafter **'Council of Europe'].**

Types and modes of cyberviolence

Cyberviolence against women and girls may involve different types of harassment, violation of privacy, sexual abuse and sexual exploitation, and bias, including direct threats of physical or psychological violence, against women and girls as individuals and as social groups. Some of the violence may not constitute a criminal offence, although many forms of cyberviolence are already encompassed by some domestic criminal law, such as traditional crimes involving violence, sexual exploitation and abuse, threats, extortion, hate crime, harassment, violations of privacy, and some cybercrimes. In all jurisdictions, however, traditional criminal law frameworks are inadequate.

Many of the forms and examples of cyberviolence discussed below are interconnected, overlapping or a combination of inter-related acts. The regional reports collectively refer to the following types of cyberviolence.[6]

a) Cyber-harassment

Cyber-harassment generally involves 'a persistent and repeated course of conduct targeted at a specific person that is designed to and that causes severe emotional distress and often the fear of physical harm'.[7] The central element is that the conduct is unwanted, even if not intended to cause distress or inconvenience to the person, although intended harm is usually the case. In such cases, the harassment is generally 'frequent or voluminous, whether it comes from one person ongoingly or from an ongoing stream of harassers acting on their own accord or under a coordinated campaign deliberately targeting the victim'.[8] It can threaten violence, but often is designed to cause embarrassment to the victim and their family, friends and colleagues. It may involve impersonation, falsehoods or online posting of sensitive information about or images of the victim.

A common component is that the violence, abuse and harassment is often sexualised and constitutes online sexual harassment, which may include 'reference to the targeted person's sexuality or sexual activity, sexualised insults and harassment, or shaming the person for their sexuality or for engaging in sexual activity ("slut-shaming"). Its purpose is to affect the dignity of a person, in particular by creating an intimidating, hostile, degrading, humiliating or offensive environment'.[9]

Two common forms of cyber-harassment are cyberbullying and the non-consensual distribution of intimate images.

i. Cyberbullying

A common form of cyber-harassment is cyberbullying, which is often associated with school-aged children. Types of cyberbullying may include cyberstalking, denigration, participation in exclusion/gossip groups, falsification of identity to post content online\'flaming', harassment, impersonation, 'outing', 'phishing', 'sexting', trickery, nasty text messages or e-mails, embarrassing photos, videos and websites. Cyberbullying can be considered as an umbrella for many online bullying activities, some of which are more severe than others and have led to sexual manipulation, non-consensual creation and distribution of intimate images or videos, extortion, self-harm, and suicide.

Sometimes, cyberbullying can be so extensive as to constitute online 'mobbing' or 'swarming', such as when large numbers of people simultaneously engage in online harassment or online abuse against a single individual. These events may involve a small group of actors who planned and co-ordinated the mobbing, **with other individuals joining in either knowingly or being misled into 'piling on' without awareness of the full context (that is, 'negative' bystanders).** The cyber world is part of the real world and cannot be viewed as separate and apart, as bullies possess similar motives for their deliberate and hostile behaviour that are multiple and complex. They intentionally inflict harm and put fear into others under the cloak of anonymity, as cyberbullying is often covert in nature.

6 *Africa Report*, pp. 4–30 (within the context of individual country analysis); *Asia Report*, pp. 1–5, 11–27 (within the context of individual country analysis); *Caribbean and Americas Report*, pp. 2–9, 15–22 (within the context of individual country analysis); Europe Report, pp. 8–15 (within the context of individual country analysis); Pacific Report, pp. 1–6, 6–12 (within the context of individual country analysis).

7 Council of Europe, as quoted in *Caribbean and Americas Report*, p. 4.

8 Women's Legal Education and Action Fund, as quoted in *Caribbean and Americas Report*, p. 4.

9 Dubravka Šimonović (2018), Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, UNHRC, 38th Sess, UN Doc A/HRC/38/47 (2018), p. 40.

ii. Non-consensual distribution of intimate images

Another common form of cyber-harassment is the non-consensual distribution of intimate images – often colloquially referred to as 'revenge porn' – which is sent with the aim of harassing, shaming or ruining the reputation of the targeted individual. It is usually directed at adults or teenaged persons. In some cases, the distributed video or image is of a physical sexual assault, which can doubly victimise the individual. In other cases, the distributed content consists of consensual sexual acts, forwarded or posted without the victim's authorisation. It should be noted that the victim's consent to engage in the sexual acts, to their recording, or to consensual distribution to an intended recipient (that is, 'sexting') should not be considered as consent to any further distribution of the images to other third persons.

The term 'revenge porn' has been criticised as inaccurate. First, it embeds the incorrect notion that the victim has done something 'wrong' for which the perpetrator seeks 'revenge' and, second, the purpose of the distribution is not pornographic in the sense of seeking sexual arousal but rather is an act of misogynistic violence, power and control.[10]

b) ICT-related violations of privacy

Some forms of cyberviolence are primarily related to violation of a person's privacy, including the misappropriation, revealing or manipulation of intimate data, as well as the distribution of such personal data ('doxing'), or acts such as 'cyberstalking' or 'sextortion'. The non-consensual distribution of intimate images (discussed above) is also a form of privacy violation.

i. Cyberstalking

Cyberstalking, which is similar to and often overlaps with cyberbullying, can occur in a multitude of behaviours, including using personal information about the person to threaten or intimidate, sending repetitious messages that are hostile or threatening in nature, and impersonating a person by obtaining log-in information for e-mail accounts and networking pages, and posting fake messages on the other person's account. Like stalking in the physical world, cyberstalking is often perpetrated by intimate partners or suitors, and often occurs in the context of domestic violence as a form of coercive control.

Cyberstalking can also involve the interception of private communications, such as surreptitiously hacking into a person's electronic devices or accounts and obtaining personal information involving e-mail or text content, videos, photographs, as well as metadata of a person's browsing history, phone call and texting history, and social media activity.

Intimate images or recordings may also be captured through technology-facilitated voyeurism, which involves surreptitiously observing or recording someone while they are in a situation that gives rise to a reasonable expectation of privacy (whether the person is in a private, semi-public or public space). This includes spying on someone engaged in sexual activity or in an intimate setting (for example, their bedroom) and can also include taking photos or recordings, even in a public place, of a person's body (for example, 'upskirting' or 'downblousing') in situations where that person has a reasonable expectation of privacy of the portions of the body recorded.

ii. Doxing

This conduct involves the releasing of an individual's personal information online against his or her wishes. It has commonly been used against women, at times because they opposed sexism or turned down sexual advances online. It can be particularly harmful for persons who are in or escaping from situations of intimate partner violence, or who use pseudonyms due to living in repressive regimes or to avoid harmful discrimination for aspects of their identity, such as being transgender or a sex worker.[11]

iii. Impersonation and image manipulation

In addition to hacking into and taking over social media accounts, as discussed above, perpetrators may also create fake social media accounts purporting to be the targeted person in order to impersonate them, with the intent to ruin their reputation or relationships.

10 *Caribbean and Americas Report*, p. 6; *Pacific Report*, pp. 3–4.

11 *Caribbean and Americas Report*, p. 6; *Europe Report*, p. 13.

Another form of impersonation is image manipulation, achieved through 'deepfakes', 'cheap fakes' and 'shallow fakes'. A deepfake is the use of artificial intelligence to produce videos that include false but realistic images of an individual saying or doing something that they did not say or do. For example, they may involve manipulating a pornographic video to replace the actress's face with the face of an ex-partner, celebrity or another real woman, creating what looks like real pornography featuring that person. Cheap fakes or shallow fakes attempt to achieve the same purpose, but use less sophisticated technology, such as Photoshop edits or basic video editing software.

iv. Sextortion

Where information, photographs or videos have been obtained or created, as in the previous types of cyberviolence, or otherwise obtained with or without consent, and the perpetrator attempts to sexually extort another person by threatening to distribute such material without consent '**unless** the targeted person pays the perpetrator, follows their orders, or commits sexual acts with or for them, the abuse is often referred to as **sextortion'**.[12] The motivation for such conduct may be revenge, humiliation or monetary gain, and may also include a threat to hurt the targeted person's family or friends if sexual activity is not undertaken.

c) Online sexual exploitation and sexual abuse

This type of cyberviolence often involves various forms of sexual exploitation and sexual abuse of children. Information and communication technologies (ICTs) have increased the accessibility to children by persons seeking to sexually abuse and exploit them, facilitate sharing of images and videos of sexual abuse, and contribute to making easier commercial gains from sexual exploitation. Online sexual exploitation and sexual abuse includes the behaviours listed in articles 18–23 of the *Lanzarote Convention*[13] and article 9 of the *Budapest Convention*[14] when conducted in an online environment or otherwise involving computer systems. These behaviours include: sexual abuse, child prostitution, child pornography, corruption of children and solicitation of children for sexual purposes.

The *Commonwealth Model Law on Computer and Computer Related Crime*,[15] and the model law and policies of the Caribbean HIPCAR project,[16] contain model law provisions that incorporate the essential characteristics of the crimes contained in the Budapest Convention .

d) ICT-related hate crime

Various forms of speech or expression can constitute a form of cyberviolence. These include violent, abusive or harassing expressions by means of written, audio, image- or video-based or other multimedia expression. These statements or content, which convey misogynistic or harmful attitudes towards women, girls and other marginalised identities, may meet the legal definition of hate speech in some jurisdictions. Of additional concern is that online hate contributes to radicalisation of people and leads to the risk that sympathisers of hate speech may take physical and violent action.

e) ICT-related direct threats or actual violence

Cyberviolence can also include direct threats of violence or direct violence, and can include threats to commit sexual assault, death threats, or threats to harm the targeted person's family or

12 Cynthia Khoo, "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence, Women's Legal Education and Action Fund (LEAF) (April 2021), p. 17; "Taking Action to end Violence against Young Women and Girls in Canada", Report of the Standing Committee on the Status of Women, 42nd Parliament, 1st Session (March 2017), (Marilyn Gladu, Chair), p. 34; hoc report on violence against women 2017.pdf , [hereinafter "Canadian Parliamentary Committee"].

13 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201

14 Council of Europe Convention on Cybercrime (CETS 185), http://www.coe.int/en/web/cybercrime/the-budapest-convention .

15 Commonwealth Model Law on Computer and Computer Related Crime, s. 10, https://www.thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf

16 'Cybercrime/e-crimes: Model Policy Guidelines & Legislative Texts', HIPCAR (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean), s. 13, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf

friends. Direct threats can also include interference with a person's medical devices or other critical infrastructure by means of computer hacking.

One form of direct threat is to employ false information about a person in order to put them at risk of law enforcement action in response to an alleged, but false, crime (that is, 'swatting'). Based on a false report, an emergency service is deceived to send law enforcement to a particular location, where the intended victim lives or works, to respond to a false crime (for example, homicide, bomb threat, kidnapping, etc.). The arrival of law enforcement may be terrifying and even dangerous for the victim, as there have been instances of heart attack, physical injuries and even death. The activity may be especially serious for targeted persons who are members of racialised or marginalised communities, which have historically experienced excessive use of force by police.

f) Cybercrime and other cyber manipulations

Some forms of cybercrime may also constitute cyberviolence or facilitate the commission of other forms of cyberviolence already discussed above. These include illegal access to personal data, manipulation or destruction of data, and interference with access to data, as well as computer-related fraud and forgery.

Other forms of misuse of information and communication technologies include employing means to amplify the cyberviolence attack or its harms. For example, 'co-ordinated flagging' involves 'gaming a platform's mechanisms for reporting abuse, and comprises organised activity where a large group of individuals "flag" or report someone's post for removal or account suspension, claiming it is a violation of the platform's community standards or terms of use, as a way to silence the target or cause them harm or inconvenience'.[17] Another form of misuse of ICTs is 'brigading', 'whereby skilled individuals can manipulate algorithms to 'amplify' harassment and boost harmful content'.[18] These individuals manipulate algorithms that determine what content is promoted to be received by a targeted person or by other persons searching the targeted person's name, or what content is suppressed by appearing to be less likely to be viewed. Impacts include making it more likely that certain types of harmful information about an individual are distributed. Otherwise, abusers may orchestrate mass 'downvoting' of internet posts by specific women, to prevent their words from reaching a wider audience.

These types of activity, often involving many persons as perpetrators, facilitators or audience, are relevant to the present Commonwealth report with its particular focus on **bystanders**.

Intimate partner and dating violence

Although this is not a distinct form of cyberviolence, the various forms of cyberviolence previously discussed often occur within the context of dating and intimate partner violence, abuse and harassment. Such violence merits particular mention because in this context, perpetrators 'use social media and other digital platforms and communications technologies to intimidate, isolate, and control their partners or former partners, including leveraging their own social networks to target the victim/survivor, while threatening, co-opting, and undermining the victim/survivor's own social networks as a means of further control and isolation'.[19] This coercive control sits within the broader context of patriarchal gender inequality.

Incidence of cyberviolence

All regions reported a high incidence of cyberviolence, especially as against women and girls. The rates vary due to lack of consistency in survey or statistical data, or low internet inter-connectivity in a particular country.[20] The reports refer to various international studies, as well as some local studies. While all findings could not be summarised in this report, some noted findings of the breadth of the problem are as follows:

- Africa: An international study of 51 countries surveying 4,561 women found that 85 per cent had witnessed online violence and harassment, while 54 per cent knew the

17 As quoted in *Caribbean and Americas Report*, p. 8.
18 Canadian Parliamentary Committee, p. 34.
19 As quoted in *Caribbean and Americas Report*, pp. 8–9.
20 *Africa Report*, pp. 1–2; 11–29 (in the context of individual country analysis); *Asia Report*, pp. 2–4, 11–27 (in the context of individual country analysis); *Caribbean and Americas Report*, pp. 9–12; *Europe Report*, pp. 5–7; *Pacific Report*, pp. 5–6.

perpetrator. Africa and the Middle East led for women who had witnessed online violence, with 91 and 98 per cent respectively,

- Asia: Women and girls were found to be more likely to be victimised, with cyberviolence increasing during the COVID-19 lockdowns. In India, 90 per cent of cyberstalking victims were women. Online violence against women and children was the second largest form of gender-based violence in Sri Lanka; 40 per cent of women in Pakistan had been victims of online harassment; and the proportion of adolescents cyberbullied in Malaysia was between 26 and 33 per cent.
- Europe: More than half of the 14,000 15- to 25-year-old women interviewed from 22 countries said they had been cyberstalked, sent explicit messages/images or abused online. Forty-five (45) per cent of domestic violence victims in the UK reported experiencing some form of abuse online during their relationship and 48 per cent experienced it from an ex-partner.
- Caribbean and Americas: There had been an 88 per cent increase in Canada in the reporting of sextortion and other online exploitation since the COVID-19 pandemic began. Twenty-five (25) per cent of Canadian parents had come across inappropriate behaviour online aimed at their child. About 40–43 per cent of high school students in Jamaica had been contacted inappropriately online by persons unknown to them. In Trinidad and Tobago, females were at a higher risk of being victims to unauthorised access and cyberbullying (54.3 per cent female; 45.7 per cent male), with younger age groups having a higher probability of being harassed.
- Pacific: The same forms of gender discrimination in social, economic, cultural and political structures were found to be reproduced and perhaps exacerbated in the online sphere.

Impact of cyberviolence

While cyberviolence is committed against both males and females, it has a disproportionate impact on women and girls, both in terms of its rate of incidence and impact. This is particularly the case where there is also intersectionality of race, ethnicity, religion, sexual orientation, poverty, disability and/or other socio-economic factors that marginalise them.[21] In some situations, cultural and traditional practices that are harmful to or discriminate against women and girls may accentuate the disproportionate impact.[22]

Loss of reputation and other resulting consequences from cyberviolence have psychological, physical and socio-economic impacts on victims/survivors. It can lead to social withdrawal, physical and psychological illness, low self-esteem, and may cause ill effects on their familial, social and employment relationships, sexual and psychological integrity, autonomy, equality and privacy. Cyberviolence can lead to social ostracisation and isolation, physical illness, and emotional and psychological trauma, including damaged self-esteem, a loss of self-worth, feelings of sadness and anger, anxiety, fear for personal safety, social withdrawal, and depression. In the most serious of cases, it can lead women and girls to commit self-physical harm, including suicide.

Often what occurs online can have significant consequences in the real physical world, and the distinction between cyberspace and real space is virtually meaningless. Use of social media by youth is an intrinsic part of their lives, including its use as their main means of communication. What happens in cyberspace is also carried through to physical space, and vice versa, such that both are considered 'real space' by young people. **Bystanders** can accelerate and accentuate the online and offline effects and harms of cyberviolence.[23]

Bullying and cyberbullying can also jeopardise socialising with peers and learning, resulting in a loss of interest in school activities, more absenteeism, tardiness and truancy, and lower-quality schoolwork and grades. Misogynistic and sexist expression in social media has also been evidenced in professional schools, such as law and medicine, and in the arena of pop culture.

21 *Africa Report*, pp. 1–2, 11–29 (in the context of individual country analysis); p. 31.; *Asia Report*, pp. 2–5, 11–27 (in the context of individual country analysis); *Caribbean and Americas Report*, pp. 9–15; *Europe Report*, p. 1; pp. 5–9; *Pacific Report*, pp. 1–6. These references also apply to all impacts of cyberviolence, as described subsequently in this section of the present report.

22 For example, *Africa Report*, p. 31. And see footnote 19, above.

23 For example, *Asia Report*, p. 11; *Caribbean and Americas Report*, pp. 13–14; *Pacific Report*, p. 6.

Additionally, cyberviolence can negatively affect women's and girl's public and democratic participation in society, and can relegate them to secondary status, both online and offline in society in general. This is because they feel dissuaded or fearful from participating in democratic/public activity and enjoying true and equal protection of their human rights and fundamental freedoms, including the right to freedom of expression. This denial of full democratic participation is particularly acute with professional women, such as journalists, politicians, academics, artists, activists, human rights advocates and feminists. They are targeted precisely because of their public presence and the exercise of their freedom of expression.[24]

Last, victims/survivors of cyberviolence also bear the economic costs of instituting legal actions to remove offensive material and to seek judicial remedies for the harm caused.

Bystanders

Online violence often involves three participants: perpetrators, victims/survivors, and bystanders. Bystanders play a significant role in perpetration, aggravation and mitigation of online violence. A bystander is an individual who observes an act of cyberviolence but may not be directly involved in its commission. Nevertheless, they have the choice to intervene through words or actions/non-action, to: 1) interrupt or condemn the harmful behaviour, report it to IT administrators, teachers, parents or law enforcement, or console/defend the victim/survivor (that is, 'positive' bystanders); 2) facilitate and exacerbate the harmful behaviour by providing encouragement or approval to the perpetrators or others, and/or degrade and attack actively the victim/survivor (that is, 'negative' bystanders); or 3) do nothing but view what is on their computer/mobile phone screen (that is, 'innocent' bystander). Even if the individual does nothing but passively views and takes no positive or negative action (an 'innocent' bystander), their inaction may have the effect (through a perceived silent assent/condoning) of reinforcing the behaviour of the perpetrator and exacerbating the harm caused to the victim/survivor who may feel helpless and defenceless. Thus, 'innocent' bystanders are not totally 'innocent' of moral blame or causation/contribution of harm. However, whether that inaction should result in criminal or civil liability, and/or instead instigate other social/psychological responses by society, raises fundamental philosophical, moral, political and legal questions that need to be considered.

Various factors contribute to the bystander phenomenon including the ubiquity of online social interaction, frequent anonymity of perpetrators, a 'code of silence' by victims and bystanders who are reluctant to report due to fear of retaliation or disapproval by others, age and social group dynamics, the socio-economic environment, and cultural attitudes and situational influences. These factors are also exacerbated by the psychological phenomenon of the 'bystander effect', which prevents/dissuades bystanders (whether in the offline or online sphere) from intervening, especially in situations where the number of bystanders/witnesses increases. The result is that it is less likely for any one of them to intervene due to diffused responsibility among many witnesses, and to pluralistic ignorance that something wrong and harmful is happening because others are not responding or to pluralistic ignorance as to whether anyone else has responded.[25]

Challenges in responding effectively

All regional reports noted significant challenges to effectively addressing cyberviolence, including: formal and informal institutional factors; legal and constitutional limitations; lack of sufficient action by educational and other public organisations, private sector organisations and the media; societal, cultural and religious norms; social media/online culture and behaviour; political inaction or active discrimination; lack of empathy, understanding and expertise among justice actors (the police, prosecutors, defence counsel and the judiciary); and insufficient ratification and implementation of international treaties and instruments.[26]

24 For example, *Asia Report*, p. 11; pp. 14–15; p. 23; *Caribbean and Americas Report*, pp. 13–14; *Pacific Report*, p. 5.

25 *Africa Report*, pp. 2–3; *Asia Report*, p. 5; *Caribbean and Americas Report*, pp. 14–16; *Europe Report*, pp. 2–4; *Pacific Report*, pp. 13–18.

26 *Africa Report*, pp. 1–3; p. 31, 33; *Asia Report*, pp. 6–10, 28–33; *Caribbean and Americas Report*, pp. 2–3, 22–23; *Europe Report*, pp. 23–25, 18–22; *Pacific Report*, p. 1; pp. 27–28.

3. Responses to Online Violence

Legal responses

This section will provide only a high-level summary of the existing legal framework within Commonwealth jurisdictions, as well as new law reform proposals. A detailed analysis can be found in each of the Commonwealth regional reports, as indicated within.[27] Rather, this report will attempt to posit some common denominators and characteristics of current Commonwealth legal frameworks, actual and proposed.

Some of the cyberviolence discussed above may not constitute a criminal offence, although many forms of cyberviolence are already encompassed by some domestic criminal law, such as traditional crimes involving violence, sexual exploitation and abuse, threats, extortion, hate crime, harassment, defamation, violations of privacy, and some cybercrimes. Nonetheless, in all jurisdictions, traditional criminal law frameworks are inadequate. In some instances, limitations in constitutions and human rights laws may permit some forms of discrimination, which can lead to violence against certain members of society, in particular women and girls.[28]

To various degrees, the current legal frameworks within Commonwealth jurisdictions, comprising both traditional and new enactments, may apply to criminalise some forms of cyberviolence or provide civil remedies, especially regarding such violence against women and girls. However, significant gaps exist in many, if not most, jurisdictions, as compared with those jurisdictions that have a more robust legal framework that can be applied to address cyberviolence.

Some jurisdictions have enacted (or have proposed) specific new criminal offences and statutory civil remedies to address some forms of cyberviolence, such as cyber-harassment/-bullying/-stalking, intimidation, the non-consensual recording and/or distribution of intimate images,[29] identification theft and fraud, access to personal data, sextortion, and sexual exploitation. Some other jurisdictions, meanwhile, have proposed to enact more comprehensive legal remedies.[30]

The definitional elements of many of these new offences often overlap with other existent domestic offences or vary among Commonwealth jurisdictions' definitions of offences, even within the same region, with some jurisdictions requiring definitional elements that are not required by other jurisdictions, or vice versa. Thus, there is a lack of consistency in the criminological rationale and definition of these new offences within the Commonwealth. This can hinder international co-operation by legal and judicial authorities due to a lack of common understanding as to what constitutes a crime, or due to an inability to satisfy 'dual criminality' requirements if required in order to provide assistance.[31]

Some of the laws or proposed reforms within the Commonwealth are, or appear to be, limited to online 'cyber' (computer) activity, while others are broader and encompass any electronic communication. However, as distinctions are often artificial or meaningless as between the physical world and the cyber realm, these laws and proposed reforms should be technologically neutral (that is, not restricted to computer systems and the 'cyber' electronic realm, or to electronic/telecommunications), to the greatest extent possible, as similar violence often occurs in both the offline and online spheres, or originates in one sphere and is carried through into the other.[32] Violence against women and girls needs to be addressed comprehensively, both offline and online.

27 *Africa Report*, pp. 4–30; *Asia Report*, pp. 11–27; *Caribbean and Americas Report*, pp. 15–22, 28–33; *Europe Report*, pp. 9–15, 18–22; *Pacific Report*, p. 2; pp. 6–12.

28 For example, *Africa Report*, p. 10, 13, pp. 15–16, p. 19, 30; for the contrary, see p. 18, pp. 21–22; 25–26.

29 Ibid.

30 Ibid.

31 Ibid.

32 For example, *Africa Report*, pp. 8–15, p. 27; *Asia Report*, pp. 7–9; *Caribbean and Americas Report*, p. 19, 29; *Europe Report*, p. 4.

Some of the crimes described in *the Commonwealth Model Law on Computer and Computer Related Crime*[33] ('the Model Law') may address some forms of cyberviolence, and several jurisdictions have enacted legislation that aligns with the Model Law. Nevertheless, conformity in domestic law with the Model Law is not in itself sufficient to address the more complex problem of cyberviolence, especially as against women and girls.

Traditional common law torts, such as the law of defamation, may also apply to provide some civil redress. Recent advances have occurred in some regions regarding the judicial development of new tort remedies, which would address some forms of cyberviolence, such as harassment and the distribution of private images and data, and defamation,[34] while criminal, civil and regulatory law reforms have been proposed in several jurisdictions.[35]

Some jurisdictions have enacted statutory criminal/civil law provisions concerning defamation or other menacing/indecent/offensive communications that cause harm or distress. However, several of these laws have been criticised due to their breadth of scope and negative impact on democratic and freedom of expression.[36]

With respect to online **bystanders** (as discussed earlier above), some may be passive observers ('innocent' bystanders), who either unwittingly come across and view, or intentionally seek out, the posted, offensive material, but otherwise do nothing more than passively view/witness it and then terminate their viewing without providing any comments, encouragement, opposition or other response such as further transmission and distribution. Other bystanders may be recruited by perpetrators, or act on their own accord, to intentionally or recklessly further the cyberviolence, or unwittingly, or be misled to, further distribute the communication without full awareness of the harmful context or harmful impact. These bystanders are essentially 'non-innocent' bystanders, but their degree of moral or legal culpability may vary depending on the circumstances and the nature of their action or inaction, such that they are either 'positive' or 'negative' bystanders, or some status in between.[37] It is, therefore, important that any legal, educational and preventative measures recognise the various distinctions in the level of moral responsibility and legal culpability of bystanders.

With respect to criminal liability of **bystanders**, some jurisdictions have clearly articulated statutory rules in penal codes, or cybercrime laws, regarding participation in general in the commission of any criminal offence, while other jurisdictions rely on common law principles and jurisprudence. Based on the application of these general rules and principles, and depending on the circumstances, the person's conduct and their level of mental awareness (that is, their intent, knowledge or recklessness), both perpetrators and some bystanders could be criminally liable as parties to a criminal offence that involves acts of cyberviolence. Depending on the circumstances, a bystander could be criminally liable as a party to the offence by way of being a co-principal (co-perpetrator), an aider or abettor, facilitator, or an inciter or procurer.[38]

Law reforms have been proposed in some jurisdictions regarding the role and regulation of social media and ICT platforms. In one jurisdiction, law reforms have been proposed to create a new statutory tort and civil remedies to address the non-consensual distribution of intimate images, and to reform the tort law of defamation and court process in light of the internet age.[39]

One regional report has extensively examined the proposal to enact 'Good Samaritan' and 'Bad Samaritan' laws in relation to **bystanders**. The former, while not imposing any duty to intervene, would provide a statutory limitation for liability in relation to the good faith efforts of any prospective rescuer or intervener, including attempts to dissuade or cease the continued commission of the offensive conduct, or notify law enforcement or other emergency services.[40] In the physical world, some Australian jurisdictions have enacted laws in relation to assisting a person

33 Commonwealth (2017), https://www.thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf.
34 For example, *Caribbean and Americas Report*, pp. 20–22; *Europe Report*, pp. 14–15.
35 For example, *Caribbean and Americas Report*, pp. 28–33.
36 For example, *Asia Report*, pp. 21–22; *Caribbean and Americas Report*, pp. 18–19; *Pacific Report*, p. 7.
37 See section above, in Part II on 'Bystanders'.
38 *Africa Report*, pp. 2–3, p. 23, 26, 28; *Asia Report*, pp. 33–35; *Caribbean and Americas Report*, pp. 15–16; *Europe Report*, p. 2; *Pacific Report*, pp. 13–14.
39 For example, *Caribbean and Americas Report*, pp. 28–33.
40 *Pacific Report*, p. 19. See also *Africa Report*, p. 32; *Europe Report*, p. 12.

who is apparently injured or at risk of being injured or otherwise requires emergency assistance. It is uncertain whether such laws would apply to online cyberviolence and, even if they did apply, whether that would provide sufficient motivation for intervention by bystanders in the current online social environment.[41]

The same regional report has also examined the pros and cons of enacting 'Bad Samaritan' laws; that is, legislation that 'seeks to penalise those who witness and have an opportunity to intervene, directly or indirectly, in support of those in need of rescue, or who are otherwise in an apparent state of distress, but who fail to do so'.[42] After examining the moral, political and other philosophical arguments in favour or against such a legal regime addressing non-action, nonfeasance or malfeasance, the report examines the rationale for such proposed legislation and whether the criminal law is an appropriate vehicle to encourage positive behaviour and impose punishment for failure to act benevolently. Several challenges in enacting such legislation are also examined, including defining when the duty would be triggered, who (among possibly many, if not hundreds, of bystanders) would be bound to intervene, what would be the required response, and the various law enforcement and prosecutorial challenges involved within an online, cultural environment that drives online violence or facilitates bystanders to exacerbate it intentionally or unwittingly.[43] At least one jurisdiction has enacted an obligation on ICT service providers to notify various authorities of the presence of child pornography that they find on their service platforms.[44]

Last, one needs to question whether the enactment of such 'Samaritan' legislation, with its own definitional challenges and limitations, would really add much to the existing legal framework (discussed above) regarding co-perpetrators, parties, and aiders and abettors, facilitators, etc., which already differentiates bystanders who passively observe, encourage, facilitate or further disseminate, or take action to dissuade or report the criminal activity to law enforcement authorities. 'Positive' bystanders are likely not criminally or civilly liable, as their actions are intended to cease or dissuade the offensive conduct or provide relief to the victim/survivor. 'Negative' bystanders are likely covered by existing criminal, common law principles and/or statutory provisions concerning secondary participation in an offence. Responses, whether legal or programmatic, to the purely passive, 'innocent' bystander raise philosophical, moral, legal and practical questions as to how to respond appropriately and effectively. This issue requires further examination.

In conclusion, most Commonwealth jurisdictions could benefit by examining the criminal and civil enactments, or proposed law reforms, of the jurisdictions that have acted comprehensively. In addition, the Commonwealth Secretariat could assist jurisdictions in achieving some consistency in the criminological and civil redress rationales and definitions of criminal offences and civil remedies.

Programme responses

While individuals (whether perpetrators, co-perpetrators, or aiders and abettors, etc.) should be held accountable by criminal and civil laws for their conduct, the root causes of the conduct are systemic social and cultural norms involving equality-based human rights issues. While these social and cultural norms vary across Commonwealth jurisdictions, they do not justify actual or threatened violence, harassment or bullying of victims/survivors, whether such conduct be online or offline. To address cyberviolence meaningfully, and especially the disproportionate impact on women and girls, requires jurisdictions to undertake social transformation to address the negative culture of misogyny, sexual exploitation, gender-based stereotypes and discrimination, discrimination against sexual orientation, racism, discrimination against minority groups, and other intersecting socio-economic factors that have historically disadvantaged the achievement of equality.[45]

Responses to address cyberviolence vary across the Commonwealth, with some jurisdictions being more active than others.[46] Some

41 *Pacific Report*, p. 19.
42 *Pacific Report*, p. 21. See also *Africa Report*, pp. 31–32.
43 *Pacific Report*, pp. 22–26.
44 For example, Canada, *Caribbean and Americas Report*, p. 20.
45 *Africa Report*, pp. 1–2, p. 31; *Asia Report*, pp. 1–3; *Caribbean and Americas Report*, pp. 12–14, p. 34; *Europe Report*, pp. 5–7; *Pacific Report*, pp. 1–6.
46 *Africa Report*, p. 2, and see pp. 4–30 (in the context of individual country analysis); *Asia Report*, p. 10, 12, 13, pp. 17–20, 22–23, 24–26; *Caribbean and Americas Report*, pp. 24–28; *Europe Report*, pp. 26–27; *Pacific Report*, pp. 27–28.

jurisdictions have implemented programmes developed by law enforcement, government, community organisations or the ICT industry, and some jurisdictions have conducted extensive parliamentary studies and reports[47] with recommendations for action to address cyberviolence against women and girls. All of these programmes have the goal of raising awareness of the problem and its impact, creating a positive culture of digital citizenship and responsibility, whereby users of social media and ICTs understand and exercise their rights to safe, responsible and inclusive online communities as providers, citizens and consumers.[48] Some of the programmes promote awareness of the problem, positive online behaviour, equality, diversity, human rights and empathy, and some empower counter-narratives to sexist and misogynistic messages.[49] Some research studies and programmes are specifically directed to create 'positive' **bystanders**, whereby online viewers are encouraged to intervene, defend targeted persons and report incidents as appropriate.[50] Many of these programmes involve social-psychological research and educational programmes, which are not within the purview of the mandates of law ministers, but of other government ministries.

Instead of summarising in detail the various, historical and current programmatic efforts that have been undertaken, which can be found in detail in the various regional reports, this current report will instead (based on the Commonwealth experience), propose in Part IV some forward, action-oriented programme proposals for consideration by relevant stakeholders in their jurisdictions.

The role of ICT companies/ platforms

a) Liability of digital platforms

There are several laws within Commonwealth jurisdictions that could theoretically establish civil or criminal liability for digital platforms, depending on the circumstances and involvement of the ICT.[51] Such laws include copyright laws, criminal laws addressing non-consensual distribution of intimate images, harassment or hate speech (depending on the level of knowledge and awareness by the ICT), statutory human rights laws, product liability laws, and defamation laws (where the ICT had specific knowledge of the defamation but took no action to address it). Generally, the risk and degree of liability rises the more the platform is involved in the activity and abandons its 'innocent' **bystander** status – that is, its intermediary-infrastructure role of merely connecting third parties together.

Even where an ICT company/platform is not a party to an offence or a defendant in a civil action, it may be subject to various statutory or judicial obligations, such as forwarding a notice, identifying users, and de-indexing or disabling access to content.

While various laws may apply to them, online platforms remain largely unregulated in the Commonwealth, although some jurisdictions have enacted some regulatory measures or are considering doing so.[52]

b) ICT measures to address cyberviolence

In response to public pressure, many ICT companies/platforms have implemented policies and measures to respond to cyberviolence, including updating technology to remove harmful material and dedicating more human resources to review and remove content. Additionally, these companies have been working with other organisations, including law enforcement, to develop technologies that identify harmful content and prevent customers from accessing certain harmful websites. Other technologies provide education, via text messages to youth, to teach acceptable online behaviour and empower counter-narratives to sexist and misogynistic messages, instead spreading messages promoting equality, diversity, human rights and empathy.[53]

47 For example, *Caribbean and Americas Report*, pp. 26–27.
48 For example, *Caribbean and Americas Report*, pp. 24–25; *Pacific Report*, pp. 27 –28.
49 *Africa Report*, p. 2, and see pp. 4–30 (in the context of individual country analysis); *Asia Report*, p. 10, 12, 13, pp. 17–20, 22–23, 24–26; *Caribbean and Americas Report*, pp. 24–28; *Europe Report*, pp. 26–27; *Pacific Report*, pp. 27–28.
50 *Africa Report*, p. 2; *Asia Report*, pp. 33–35; *Caribbean and Americas Report*, pp. 26–28; *Europe Report*, pp. 26–27; *Pacific Report*, p. 16, pp. 27–28.
51 *Africa Report*, p. 12; *Caribbean and Americas Report*, p. 22.
52 *Africa Report*, p. 12, 15, 17, 18, pp. 20–21, p. 22, 24, 30; *Asia Report*, p. 10, 20, 24, 26, 28, pp. 31–32; *Caribbean and Americas Report*, pp. 22–23, 30–31; *Europe Report*, pp. 23–24; *Pacific Report*, pp. 16–18.
53 Ibid.

While it is important to hold ICT companies/platforms accountable, this must be done in such a manner as not to incentivise these companies to make protective business decisions that result in unwarranted censorship of important political and social speech/expression. Any regulatory framework must balance human rights and protection of freedom of expression.[54]

Clearly, while ICT companies/platforms are a major part of the problem in distributing cyberviolence, they are also part of the solution to creating a positive digital citizenship for all providers and users, including online **bystanders**.

54 *Caribbean and Americas Report*, p. 23.

4. Conclusions

This part contains two sets of conclusions. As this report was initially presented to Commonwealth law ministers at their meeting in Zanzibar in 2024, Part A of this section presents a synthesis of the major recommendations from the five regional reports, and contains many recommendations that are not within the scope of expertise or domestic legal/policy mandates of law ministers. As the responsibility for many of these matters lies with other government ministers and their departments, or the non-governmental sector, it is difficult for law ministers to take decisions on these matters. Nevertheless, these matters are part of a comprehensive strategy to address violence against women and girls, which also includes legal and justice matters. Part B contains several recommendations upon which law ministers can take decisive action, given their expertise and domestic legal/policy mandates within their governments.

a) 'Commonwealth Action Plan to address Cyberviolence, in particular Online Violence Against Women and Girls'

From an analysis of the five Commonwealth regional reports, the following *Commonwealth Action Plan* can be distilled as a guide to address cyberviolence, especially as against women and children, (including the role of **bystanders**).

Effectively addressing cyberviolence, especially as against women and girls, requires a holistic, multi-sectoral approach across government ministries/departments, Commonwealth jurisdictions and various branches of the Commonwealth Secretariat, all of which involves the improvement of both criminal and civil law legal frameworks, law enforcement, prosecutorial and judicial training and responses, research, public education, private sector involvement, support for victims and survivors, respect for the human rights of all members of society, and the development of various government, law enforcement and community educational programmes, including programmes by the media, to promote positive online activity and to dissuade the commission of cyberviolence, including by **bystanders**.

The *Commonwealth Action Plan* is not a directive, but rather a road map to serve as a general, illustrative guide regarding the various activities and programmes that could be implemented by government, non-governmental community organisations, the media, ICT companies, and the law enforcement, legal and health/social welfare communities. The *Commonwealth Action Plan* contains the following elements.

Research

- Research on the prevalence of cyberviolence, especially as against women and girls, using disaggregated data that acknowledges intersecting identities of participants (perpetrators and **bystanders**) and victims/survivors.
- Research on the impact of cyberviolence, especially on women and girls, employing a Gender-Based Analysis Plus (GBA+) analytical lens; that is, an analysis taking into account the gender-based and other intersecting identities (for example, age, race, ethnicity, religion, poverty, disability, minority status and other socio-economic factors, etc.) of participants (perpetrators and **bystanders**) and victims/survivors.
- Research into emerging types of cyberviolence, especially as against women and girls, and their impacts on participants (including perpetrator and **bystanders**) and victims/survivors.
- Research to better understand the different roles of perpetrators and **bystanders**, as well as their impact on each other and on victims/survivors.
- Research to examine the role of **bystanders**, how they respond online and their motivations and rationale for responding, or not. The research should also examine how to prevent cyberviolence by online **bystanders**, and how to promote positive behaviour and responsibility, through education and other preventative measures.

- Research on various social, psychological and other programmatic measures that could be employed to address cyberviolence, especially as against women and girls, and with particular regard to promoting positive behaviour and responsibility of **bystanders**.

Training and education

- Education for the general public on cyberviolence, especially with respect to women and girls, regarding its impact, prevention and available measures to seek assistance involving legal remedies, healthcare and psychological counselling.
- Education to promote a positive culture for online activity and change the harmful norms and sexist/stereotype culture that negatively influences gender relations, gender equality and violence against women and girls.
- Education directed at youth that prioritises the development of critical thinking skills toward the media and the internet, teaches concepts of digital civility (positive behaviour, rights and responsibilities), counters institutionalised social media behaviour, and distinguishes between acceptable online behaviour, unacceptable online behaviour and criminal online behaviour.
- Education regarding the role of **bystanders** in the commission of cyberviolence, and the development of strategies and programmes to educate internet users who witness cyberviolence regarding how to be 'positive' **bystanders,** so as to intervene to stop, address and report perpetrators and 'negative' **bystanders** involved in cyberviolence.
- Education for parents on how to recognise that their children may be subject to cyberviolence, and be aware of the various legal, community and health/psychological supports available to assist them and their children.
- Training and education for academic institutions, and their teachers and professors, regarding the prevalence, nature and impact of cyberviolence, and various measures that could be employed to prevent and respond to cyberviolence and physical violence and abuse against students and faculty members.
- Training and education for professionals and workers in the health/psychological care, community wellness and social welfare sectors of society, both in the public and private sectors, and the development of a public health approach in response to emerging impacts of cyberviolence, especially as regard to women's and children's psychological and physical well-being.

ICT companies

- Governments should encourage ICT companies to improve their reporting mechanisms to law enforcement agencies of known incidences of online violence against women and girls on their networks and systems. In some cases (for example, distribution of child pornography), consideration should be given to require, by law, mandatory reporting when ICT companies are aware of the abuse.
- ICT companies should develop policies and measures to respond to cyberviolence, including updating technology to identify and remove harmful material and dedicating more human resources to remove content, as well as preventing users from accessing certain harmful websites.
- ICT companies should develop educational programmes for users of their services regarding their rights, liabilities and remedies for providing and/or receiving cyberviolence and abuse, as well as to teach acceptable online behaviour and empower counter-narratives to harmful messages in order to promote equality, diversity, human rights and empathy, and to encourage reporting of abuses.

Justice sector

- Law enforcement training and capacity building to develop better understanding of the commission of cyberviolence, especially as against women and children, and to develop programmes to prevent cyberviolence and implement gender-sensitive responses to persons who report cyberviolence.
- Training and capacity building concerning cyberviolence, especially as against women and girls, for various justice actors – the police,

prosecutors, the judiciary and legal counsel – that is victim centred and perpetrator focused. The emphasis should be on: current and emerging types of cyberviolence crime, the impact of cyberviolence on marginalised communities, and investigative techniques; and the development of cases for prosecution, including organising the evidence required to prosecute, and strategies regarding how cases should be presented in court.

- Ensuring that laws on gender violence and equality are adequately and effectively promoted and enforced.
- Strengthening of existing justice networks across the Commonwealth to share best legal policies, laws and practices; and developing investigative and prosecutorial capacity, including joint investigation teams and mutual legal assistance.

Legal framework

- Governments should review their national legal frameworks (both criminal and civil law) to identify gaps that permit gender discrimination and the commission of cyberviolence and propose to their legislatures legal reforms to address current and emerging forms of 'cyberviolence', while balancing various rights, such as human rights and the freedom of expression. This review should, in particular, identify aspects of the legal framework that unfairly and unjustly target certain segments or members of society.
- Cultural and traditional practices should be examined, and those practices that are harmful to women and girls, and to the achievement of their equality and human rights as members of society, should be eliminated.
- Measures should be implemented to ensure that victims/survivors of cyberviolence are treated fairly and with respect, that they receive counselling and support services, and are encouraged to report such abuse and feel safe in doing so.
- Legal frameworks relating to secondary participation in criminal conduct should be reviewed to determine if law reforms would be appropriate to address the role and moral culpability of **bystanders** (such as, to incentivise 'positive' bystanders, or punish 'negative' or 'innocent' bystanders).
- As distinctions are often artificial or meaningless as between the physical world and the cyber realm, proposed law reforms should be technologically neutral (that is, not restricted to computer systems and the 'cyber' electronic realm), to the greatest extent possible, as similar violence often occurs in both the offline and online spheres or originates in one sphere and is carried through into the other. Violence needs to be addressed comprehensively, both offline and online.
- Governments should consider enacting laws addressing the obligations, liabilities and immunities of various types of internet service providers. Any regulatory framework must balance human rights and protection of freedom of expression.
- If they have not already done so, governments should undertake the necessary measures and legal reforms required in order to become parties to and ratify the international conventions relevant to addressing violence against women and girls, as well as implement other relevant international standards and norms.

b) Recommendations for action by Commonwealth law ministers

Accordingly, in light of the legal and political responsibilities of Commonwealth law ministers, it is recommended that ministers:

Endorsed the '**Commonwealth Action Plan to address Cyberviolence, in particular Online Violence Against Women and Girls',** as a guide and illustrative set of multi-sectoral ideas and recommendations, to be considered by Commonwealth governments, the Commonwealth Secretariat, law enforcement and legal communities, educational institutions, health/social welfare institutions, non-governmental organisations, the media and the private sector, in order to address cyberviolence, especially as regards women and girls (including the role of bystanders in such violence).

Agreed to advise their relevant governmental ministerial colleagues of the above-noted **Commonwealth Action Plan**, with a view to consider developing and implementing holistic, multi-sectoral measures within their national and regional jurisdictions, to achieve similar action plans, in order to address cyberviolence, especially as against women and girls (including the role of bystanders in such violence).

Mandated Commonwealth Senior Officials of Law Ministers, within its sphere of expertise, and the Commonwealth Secretariat within its broader mult-sectoral sphere of expertise, respectively, to:

1. *Develop* comprehensive model laws and/or model statutory provisions (both criminal and civil) to assist Commonwealth jurisdictions to address current and emerging forms of violence and 'cyberviolence', both in the online and offline spheres, while balancing various democratic rights, such as human rights and the freedom of expression. This study should examine the various modes of participation in the commission of an offence and the possible legal responses, as well as alternative or supportive non-legal programme responses, given that some online **bystanders** are 'positive', 'negative' or 'innocent' bystanders.
2. *Undertake* a study of social-psychological research on cyberviolence, such as cyber-harassment/cyberbullying/cyberstalking, the non-consensual recording and distribution of intimate images, and other abuses. In particular, the study should examine the role of **bystanders**, how they respond online and their motivations and rationale for responding, or not. The study should examine how to prevent cyberviolence by online **bystanders**, and how to promote positive behaviour and responsibility, through education and other preventative measures. The scope of this study should not be limited to Commonwealth jurisdictions, as significant research has also been undertaken in other parts of the world, such as in Europe, the United States of America, South America and Asia.
3. Taking into account the results of the social-psychological research (noted above), *encourage and work with* Commonwealth government ministries, including those responsible for law enforcement, education, technology, and medical/social services, to develop (for both government and community organisations) social, educational and other programmes to address cyberviolence and to promote positive online behaviour and responsibility, with particular regard to **bystanders**. As a significant proportion of cyberviolence is gender related, these programmes should be developed with a Gender-Based Analysis Plus (GBA+) analytical lens (that is, an analysis that takes into account gender-based and other intersecting identities).
4. *Work together with* other international and regional organisations to address cyberviolence against women and girls.
5. *Undertake* any other relevant measures, as appropriate, within their spheres of expertise to promote and implement the **Commonwealth Action Plan**, and in particular with respect to the sections on the 'Justice sector' and 'Legal framework'.

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

D19799