Addressing Online Violence against Women and Girls in the Commonwealth Caribbean and Americas

The Role of Bystanders

The Commonwealth

Addressing Online Violence against Women and Girls in the Commonwealth Caribbean and Americas

The Role of Bystanders

The Commonwealth

Foreign, Commonwealth & Development Office

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

www.thecommonwealth.org

Published by the Commonwealth Secretariat.

Contents

Acknowledgements

The Commonwealth Secretariat acknowledges with gratitude the financial support of the United Kingdom Foreign, Commonwealth & Development Office to the Commonwealth Cyber Capability Programme.

The report on *Addressing Online Violence against Women and Girls in the Commonwealth Caribbean and Americas: The Role of Bystanders*, is part of a series which investigates the culpability of bystanders in violent act committed against women and girls on the cyberspace.

The report was authored by Donald K. Piragoff, KC, retired, formerly Senior Assistant Deputy Minister (Policy) Department of Justice Canada.

The series was prepared under the general guidance of Dr Tawanda Hondora, Adviser and Head of Rule of Law Section, Governance and Peace Directorate (GPD). Dr Nkechi Amobi, Senior Research Officer, Cyber Capability Programme GPD, led and co-ordinated the review and editorial process of the report. Ms Emma Beckles, Programme Officer, GPD and Mr. Shakirudeen Ade Alade, Programme Coordinator GPD provided valuable input while Ms Helene Massaka, Programme Assistant GPD, provided logistical and administrative support.

The team is grateful to Mrs Elizabeth Bakibinga-Gaswaga, former Legal Adviser Rule of Law Section, GPD, for conceptualising this research project.

The team is also grateful for the constructive feedback received from internal reviewers- Mr. Steve Onwuasoanya, Human Rights Adviser, Governance and Peace Directorate and Mr. Clive Lawson, Publications Assistant, Communication Division.

Abbreviations

ECA	Eastern Caribbean Areas
HIPCAR	Harmonization of ICT Policies, Legislation and Regulatory Procedure in the Caribbean
IACHR	Inter-American Commission on Human Rights
ICT	information and communication technology
LCO	Law Commission of Ontario
LEAF	Legal Education and Action Fund
TFGBV	Technology-Facilitated Gender-based Violence
ULCC	Uniform Law Conference of Canada
UNICEF	United Nations Children's Fund
UNESCO	United Nations Educational, Scientific and Cultural Organization

Executive Summary

The purpose of this report is to map the prevalence of online violence against women and girls, with a particular focus on so-called innocent bystanders and the state of laws, institutions, policies and practices within the Caribbean and Americas region of the Commonwealth (Canada).

Cyberviolence against women and girls in the Commonwealth countries of the Caribbean and Americas (Canada) is recognised as a serious problem, and measures are being taken to address it. The prevalence of cyberviolence in terms of its root causes and impacts is gender based, with a disproportionate impact on females and marginalised individuals where there is also intersectionality of race, ethnicity, religion, sexual orientation, poverty, disability and other socio-economic factors. Similar types of violence against women and girls often occur in both offline and online spheres or originate in one sphere and carried through into the other. In the most serious cases, cyberviolence can lead to physical assaults and even suicide.

Although the current legal frameworks in the Caribbean and Americas region of the Commonwealth criminalise some forms of cyberviolence or provide civil remedies, significant gaps exist in many jurisdictions, as compared with other jurisdictions that have more robust legal frameworks to address cyberviolence. Some jurisdictions have enacted specific new offences and statutory civil remedies to address some forms of cyberviolence, such as harassment/cyberbullying/stalking and the non-consensual recording or distribution of intimate images, and a few other jurisdictions have proposed to enact more comprehensive legal remedies. Some of these laws have been criticised for negatively affecting freedom of expression, due to the breadth or ambiguity of statutory language employed.

Traditional common law torts, such as the law of defamation, may also apply to provide some civil remedy. Some recent developments have occurred in one jurisdiction, Canada, 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.

With respect to online *bystanders*, some may be recruited, or act on their own accord, to intentionally or recklessly further the cyberviolence, or unwittingly further distribute the communication without full awareness of the harmful context or harmful impact. It is, therefore, important that any legal, educational and preventative measures recognise the various distinctions in the level of moral responsibility and 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 the commission of an offence, while other jurisdictions rely on common law principles and jurisprudence. 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, a facilitator or an inciter or procurer.

While individuals should be held accountable by criminal and civil laws for their conduct, the root causes are systemic social and cultural norms involving equality-based human rights issues. Meaningfully addressing the disproportionate impact on women and girls requires social transformation to address intersecting socio-economic factors that have historically disadvantaged the achievement of equality.

Programme responses to address cyberviolence vary across the Caribbean and Americas regions, with some jurisdictions being more active than others. These programmes have been developed by law enforcement, government, community organisations or the information and communication technology (ICT) industry, and at least one jurisdiction has conducted extensive parliamentary studies and reports with recommendations for action to address cyberviolence against women and girls. All of these programmes have the goal of creating positive digital citizenship and responsibility, whereby users of social media and ICT understand and exercise their rights to safe, responsible and inclusive online communities as citizens and consumers.

Further law reforms have been proposed in some jurisdictions to address and penalise various forms of cyberviolence, as well as related procedural

and judicial powers to provide remedies. Some of these proposals address the role and regulation of social media and ICT platforms, new statutory tort and civil remedies to address the non-consensual distribution of intimate images, and reform of the tort law of defamation and related court process in light of the Internet age.

The report makes recommendations to be considered by the Commonwealth Secretariat, including the role of bystanders, further legal and social-psychological research, the development of model laws and social and educational programmes to address cyberviolence.

Purpose and Scope of This Mapping Report

This report contributes to the Commonwealth Study on Violence against Women and Girls in Cyberspace. Its maps the prevalence of online violence, and the extent to which relevant laws, institutions, policies and practices in the Caribbean and Americas region of the Commonwealth address the problem.

Because of the COVID-19 pandemic, the research was conducted primarily through Internet-based sources of information. As the extent and awareness of the problem of cyberviolence varies in the Caribbean and Americas region, so does the available online material and evidence on the subject. There is significant material on physical and sexual violence against women and girls in Canada and the Caribbean region, but not so on emerging forms of online cyberviolence. In Canada, a significant amount of research on cyberviolence exists, including Parliamentary Committee reports. Although some research is available online, most of the material on Commonwealth Caribbean countries is drawn from media and opinion articles. Thus, while significant reliance has been placed on numerous, available Canadian sources, this report attempts to extrapolate much of this material to the Commonwealth countries in the Caribbean region, which share similar common law traditions. Comparative analysis of Canadian and Caribbean studies, laws, jurisprudence, policies, practices and ongoing policy discussions should be instructive for all Commonwealth jurisdictions as they undertake their analyses on how to address the problem of violence against women and girls online and engage in law and policy reform.

Although the principal focus of the Commonwealth study is on cyberviolence and so-called innocent bystanders, cyberviolence involves perpetrators, victims/survivors and bystanders, and the complex social and legal relations among them. Therefore, an analysis of this phenomenon must examine the role of all three actors in its commission, impact and prevention.[1]

Part I The Nature of the Problem of Cyberviolence

1 Overview of Cyberviolence

1.1 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, ICT. Regarding the first component, a number of international instruments define violence against women and girls.

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.[2]

Likewise, Article 1 of the Inter-American Convention on the prevention, punishment and eradication of violence against women (the Belém do Para Convention) defines violence against women as: 'any act or conduct, based on gender, which causes death or physical, sexual or psychological harm or suffering to women, whether in the public or the private sphere.'[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 ICT, acts of violence committed by means of, or facilitated by, ICTs has been defined by the Council of Europe as follows: '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] The Council of Europe's definition is gender neutral.

The Inter-American Commission on Human Rights (IACHR) declared that violence against women and girls on the Internet 'has emerged as a new form of gender-based violence which the IACHR notes is spreading rapidly and poses a significant danger'[6] in Latin America and the Caribbean. Cyberviolence that is gender based, and which is specifically directed at women and girls, is of particular gravity and social concern. A Canadian Parliamentary Committee report defined 'cyberviolence against women and girls' as follows:

> Cyberviolence involves the use of social media and information and communications technologies (ICTs) for committing an act of violence or extending an act of violence in order to harm the well-being of an individual or group. While both men and women experience violence through social media and ICTs, witnesses noted that women and girls are at greater risk than men and boys of experiencing cyberviolence, especially severe types of harassment and sexualized online abuse.[7]

Likewise, the IACHR also found that women and girls face a higher risk of cyberviolence and discrimination, such as 'stalking, grooming, threats, blackmail and sexual harassment; upload and/or dissemination of intimate images, videos, or audio clips without their consent; accessing or disclosure of their private information without their consent; upload and dissemination of modified images or videos of girls as pornographic material; creation of fake profiles, etc.'[8]

The Canadian Parliamentary Committee's report noted that acts of cyberviolence against women and girls are 'rooted in larger social and cultural problems – including sexism and misogyny – that contribute to violence against young women and girls in the offline world'.[9]

A report by the Women's Legal Education and Action Fund (LEAF) notes that '[t]echnology-facilitated gender-based violence, abuse, and harassment is part of the continuum of violence, abuse, and harassment that women and girls face in the world regardless of technology'; it is wielded as a tool 'to maintain men's dominance over women as a class, and to reinforce patriarchal norms, roles and structures', and 'is rooted in, arises from, and is exacerbated by misogyny, sexist norms, and rape culture, all of which existed long before the Internet'.[10]

While cyberviolence is similar to and rooted in the norms and values of traditional violence against women and girls, the LEAF report also notes that gender-based violence that is technologically facilitated 'in turn, accelerates, amplifies, aggravates, and perpetuates the enactment of harm from these same values, norms, and institutions, in a vicious cycle of technological systemic oppression'.[11] The IACHR notes that 'girls often find themselves in a continuum of violence both offline and online in which they feel isolated, humiliated, and emotional distressed'. Not only does technological facilitation accelerate, amplify, aggravate and perpetuate acts of harm, but it is also different from other forms of violence against women and girls. The Canadian Parliamentary Committee report[12] posited that cyberviolence is different due to the following characteristics:

- Accessibility and relentlessness. Victims can be attacked online at any hour and on any day in typically 'safe' locations, such as their homes.
- Disinhibition. Perpetrators may feel less empathy and find it easier to be cruel when they cannot see or be seen by their target.
- Audience. The online realm has a potentially huge audience.
- Anonymity. Perpetrators can use deception or anonymity to undertake their activities.[13]
- Ease of access. The automation of technology requires little technical knowledge, and the affordability of most technology provides access.
- Digital permanence. Content posted online about a person becomes a part of their permanent online identity, difficult to erase.

Having examined the general characteristics of the definition of cyberviolence against women and girls, the next section examines various types or modes of cyberviolence.

1.2 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 criminal offences, although many forms of cyberviolence are already encompassed by some domestic criminal laws, such as traditional crimes involving violence, sexual exploitation and abuse, threats, extortion, hate crime, harassment, violations of privacy and some cybercrimes. In some jurisdictions, existent criminal law frameworks are inadequate.

Some jurisdictions, such as Antigua and Barbuda, Barbados, Canada, Grenada, Guyana, Jamaica, St Kitts and Nevis, Saint Lucia, St Vincent and the Grenadines and the British Virgin Islands, have enacted laws that specifically address particular forms of cyberviolence, and some jurisdictions, such as Trinidad and Tobago, have recently proposed enactment.[14]

As an analytical framework, this section generally follows the classification system employed by the Council of Europe in its international study to map cyberviolence,[15] but with variations and additions as noted in Canadian and Caribbean experiences. The Council of Europe study is particularly relevant to the Americas experience, as representatives from Canada and the United States participated in the working group,[16] and many of the forms of cyberviolence identified are also experienced in the Caribbean and Americas region of the Commonwealth.

Many of the forms and examples of cyberviolence discussed below are interconnected, overlapping or constitute a combination of acts.

1.2.1 Cyber-harassment

According to the Council of Europe, 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'.[17]

However, the LEAF report notes that 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.[18] 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'.[19] 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 about the victim, online posting of sensitive information or images. According to the Council of Europe, the following constitute cyber-harassment:

- Unwanted sexually explicit emails or other messages.
- Offensive advances in social media and other platforms.
- Threat of physical or sexual violence.
- Hate speech, meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and/or other traits (such as sexual orientation or disability).[20]

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, sexualized insults, and harassment, or shaming the person for their sexuality or for engaging in sexual activity ("slut-shaming")'.[21]

A UN report has defined it as follows: 'Online sexual harassment refers to any form of online unwanted verbal or nonverbal conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular by creating an intimidating, hostile, degrading, humiliating or offensive environment.'[22]

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

1.2.1.1 Cyberbullying

A common form of cyber-harassment is cyberbullying, which is often associated with school-aged children. While this term is popular, some witnesses testifying before a Canadian Parliamentary Committee 'cautioned against using the term cyberbullying because it does not reflect the seriousness of the violence and because youth do not identify with the term'.[23]

The Council of Europe has summarised cyberbullying as follows:

> The literature identifies different types of cyberbullying which include cyberstalking, denigration, participation in exclusion/gossip groups, falsification of identity to post content online\flaming, harassment, impersonation, 'outing', phishing, 'sexting' and trickery. As noted by some authors, 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 ('cutting') and suicide. For this reason, *from a criminal investigation and prosecution perspective, it is essential to distinguish between the different types of cyberbullying and it is also important to distinguish between the different roles individuals play in a given act of cyberbullying*. ...
>
> Examples of cyberbullying include nasty text messages or emails, rumours sent by email or posted on social networking sites, and embarrassing pictures, videos or websites. *Cyberbullying typically involves a sustained series of such messages, whether orchestrated by a single person or a group of peers and the cumulative impact can be quite devastating*.[24]

Sometimes, cyberbullying can be so extensive as to constitute online mobbing or swarming. This occurs 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 coordinated the mobbing, with other individuals joining in either knowingly or being misled into piling on without awareness of the full context.'[25]

The italicised passages in the Council of Europe quotations above, which distinguish the different roles that individuals play in a given act of harassment, especially where there is activity of a group of peers, are in part the essence of the concept of the not-so 'innocent bystanders' (i.e., negative bystanders), which is discussed in section 5.

With respect to the conduct and motives of the perpetrators (and co-perpetrators), the Trinidad and Tobago Guardian provided a vivid and comprehensive description of cyberbullying in the Caribbean, as follows:[26]

> Cyberbullying is the label that refers to a person being wilfully and repeatedly harmed, tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted by another person through using information, communicative and electronic/digital technologies such as the Internet and mobile devices.
>
> It predominantly occurs via the Internet through emails, blogs, posts, videos on social media websites (Facebook, Twitter, YouTube, Myspace, etc.) and interactive devices (mobiles) through text messages and instant messaging. These are used to aggressively and intentionally harm someone.
>
> Cyberbullying transpires when three components intersect: teenagers, technology, and trouble. This perfect storm manifests into the wilful, repeated harm inflicted on a person using computers, cell phones and other electronic devices. Cyberbullying, an old problem in a new guise, is a serious issue in Trinidad and Tobago and is rapidly becoming an epidemic in more subtle and prevailing forms within the nation's schools.
>
> The cyber world is part of the real world and cannot be viewed separately 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 covert in nature.
>
> These cyberbullies have the need to feel empowered, popular, superior or are socially pressured by their peers or have been victims of bullying themselves. Likewise, for other cyberbullies, their motives may differ; some are often motivated by anger, revenge or frustration, others do it to defend themselves or torment others. Some even bully others for entertainment or may have done it by accident without considering the consequences.
>
> Cyberbullies deliberately harm others by name-calling, making angry/vulgar/abusive comments, sending/posting cruel/insulting messages, spreading rumours/threats, posting rude or upsetting images, revealing secrets, or embarrassing information, intentionally ignoring/excluding someone, or engaging in online impersonation–pretending to be someone else to damage the reputation of someone by stealing their password.

1.2.1.2 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.[27] 'In some cases, the distributed video or image is of a sexual assault, which can doubly victimize the individual. In other cases, the distributed content consists of consensual sexual acts, forwarded, or posted without the victim's authorization.'[28]

Regarding the former type of cyberbullying involving sexual assault, LEAF documents a number of incidents in Canada and the United States involving technology-aggravated sexual assault where men or teenage boys filmed themselves sexually assaulting a woman or girl, who was sometimes unconscious, and then posting the video or pictures on social media.[29] Such conduct is undertaken 'as a way to revictimise, humiliate and intimidate survivors' as well as being 'used by community members to bombard [victims/survivors] with threats and abuse to try to keep them from reporting and to shame them'.[30]

Intentionally uploading nude or intimate images of a person, without their consent and intending to cause that person harm, has also been noted as an emerging problem in the Caribbean, and predominantly targeting and harming females.[31]

In cases where the sexual acts are consensual, and the recorded images have also been obtained or created with the knowledge and consent of the targeted person, this consent does not include the distribution of the images to other persons.[32]

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.[33]

1.2.2 ICT-Related Violations of Privacy

Some forms of cyberviolence are primarily related to the 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.

1.2.2.1 Cyberstalking

Cyberstalking 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 email accounts and networking pages, and posting fake messages on the other person's account.[34] 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.[35]

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 email or text content, videos and photographs, as well as the metadata of a person's browsing history, phone call and texting history, and social media activity. 'Some mobile apps, known as spyware or stalkerware, are designed and marketed for the purpose of enabling their customers to systematically spy on, monitor, and track intimate partners or former partners through their mobile phones, after covertly installing the software.'[36] Sometimes, non-malicious apps, usually developed for child or employee monitoring are repurposed into spyware and stalkerware.[37]

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[38]). 'This includes spying on someone engaged in sexual activity or in an intimate setting (e.g., their bedroom) by illicitly accessing their webcam or their phone camera, without their consent or knowledge.'[39] It can also include taking photos or recordings, even in a public place, of a person's body (e.g., 'upskirting') where the person has a reasonable expectation of privacy of the parts of the body recorded. Spyware or stalkerware, as noted above, can be used to record images.

1.2.2.2 Doxing

The Canadian Parliamentary Committee heard evidence about an emerging form of cyberviolence, related to cyberstalking. This conduct is coined 'doxing', which 'involves the releasing of an individual's personal information such as pictures, social insurance number and home address' 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.[40] 'Doxing is particularly concerning for individuals who are, for example, 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.'[41]

1.2.2.3 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 to impersonate them, with the intention of ruining their reputation or relationships.[42]

Another form of impersonation is image manipulation, achieved through deep fakes, cheap fakes and shallow fakes. A deep fake 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. 'Approximately 96% of deep fakes online today 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, without their consent.'[43] 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.[44]

1.2.2.4 Sextortion

Where information, photographs or video has 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.'[45] The motivation for such conduct may also include a threat to hurt the targeted person's family or friends if sexual activity is not undertaken. 'The aggressor's motivation may also be revenge, humiliation or monetary gain.'[46]

1.2.3 Online Sexual Exploitation and Sexual Abuse

This type of cyberviolence often involves various forms of sexual exploitation and sexual abuse of children. ICTs have increased children's vulnerability to sexual abuse and exploitation, including the sharing of images and videos of sexual abuse and contributing to making easier commercial gains from sexual exploitation.[47] Online sexual exploitation and sexual abuse includes the behaviours listed in Articles 18–23 of the Lanzarote Convention[48] and Article 9 of the Budapest Convention[49] when it is conducted in an online environment or otherwise involve computer systems. These include:

- Sexual abuse (Article 18), such as engaging in sexual activities with an underaged child or engaging in sexual activities with a child where coercion or abuse of a position of trust, authority or influence is used.
- Child prostitution (Article 19), such as recruiting or coercing a child into prostitution, or having recourse to prostitution.
- Child pornography (Article 20), various activities in relation to child pornography such as: producing, offering or making available, distributing or transmitting, procuring for oneself or for another person, possessing and knowingly obtaining access, through ICT.
- Corruption of children (Article 22), such as intentionally causing, for sexual purposes, an underaged child to engage in sexual activities, or to witness sexual abuse or sexual activities, even without having to participate.
- 'Solicitation of children for sexual purposes' (Article 23) – also called 'grooming' or 'luring'.[50]

According to the IACHR within Latin America and the Caribbean there has been:

> a proliferation in the use of technologies and digital spaces for planning, recruiting the girl in order to violate them sexually or traffic them for various purposes, but in particular for the sexual exploitation and pornography. From ... information received, the IACHR notes that organized crime networks in various countries use social networks and different online communication platforms to lure girls, usually with deception, into criminal activities.[51]

The Commonwealth Model Law on Computer and Computer Related Crime,[52] and the model law and policies of the Caribbean HIPCAR project,[53] contain model law provisions that incorporate the essential characteristics of the Budapest Convention crime.

1.2.4 ICT-Related Hate Crime

Various forms of speech or expression can constitute cyberviolence. These include violent, abusive or harassing expressions by means of written, audio, image- or video-based or other multimedia expression. According to LEAF, '[s]ome perpetrators may post statements or other content that conveys such misogynistic or harmful attitudes towards women, girls and other marginalized identities, that they meet the legal definition of hate speech'.[54] Of additional concern is that online hate contributes to the radicalisation of people and leads to the risk that sympathisers of hate speech may take physical and violent action.

A Canadian Parliamentary Committee conducted a significant study on online hate, including hate directed at sexual orientation, and gender identity or

expression, as well as at age, race, national or ethnic origin, religion, mental or physical disability, etc.[55]

As online hate is a discrete, significant subject that is well researched and broader in scope than only targeting women and girls and other gender biases, a full mapping of this issue is not feasible within the mandate of the present mapping exercise.

1.2.5 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 or threats to harm the targeted person's family or friends.[56] Direct threats can include 'interference with medical devices causing injuries or death, or attacks against critical infrastructure by means of computers'.[57]

One form of direct threat is to employ false information about a person with the objective of putting them at risk of law enforcement action in response to an alleged, but false, crime:

> 'Swatting' is an example of how computer systems can be misused for many types of conduct with violent impact on victims. It is the use of telephones and often computer systems to deceive an emergency service in order to send law enforcement to a specific location based on a false report. The name comes from the acronym 'S.W.A.T.' (Special Weapons and Tactics) which are law enforcement units that have specialised training and may employ military-style equipment. False reports include reporting homicides in someone else's home, bomb threats, and kidnapping. ...
>
> Swatting may be terrifying and dangerous to the victims, who have been killed by responding law enforcement officers or who have suffered physical injuries such as bullet wounds and heart attacks.[58]

The activity may be extremely dire for targeted persons who are members of racialised or marginalised communities, which have historically experienced excessive use of force by police. It can also be combined with other forms of cyberviolence, such as threatening to 'swat' a targeted person unless they comply with a request, such as sending nude photos to the perpetrator, or in retaliation for a woman's political views expressed online.[59]

1.2.6 Cybercrime and other Cyber Manipulations

Some forms of cybercrime may also constitute cyberviolence or facilitate 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.[60]

Other forms of misuse of ICT include employing means to amplify the cyberviolence attack or its harms. For example, coordinated 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'.[61] Another form is 'brigading', 'whereby skilled individuals can manipulate algorithms to "amplify" harassment and boost harmful content'.[62]

Individuals can also 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 or 'abusers may orchestrate mass "downvoting" of posts by specific women, to prevent their words from reaching a wider audience'.[63]

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

1.2.7 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. It 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'.[64] This coercive control 'sits within the broader context of patriarchal gender inequality, which includes sexist and heterosexist social norms, gendered structural inequality, and the traditionally male-dominated digital media industry'.[65]

2 Available Data on Cyberviolence

2.1 Statistics

A survey of approximately 14,000 girls (aged 15–25 years) in over 20 countries revealed that 58 per cent had been harassed or abused online.[66] Unfortunately, few Caribbean countries were surveyed.[67] Significant research has been done in the Caribbean and Americas region on violence against women and girls, but only a few focused primarily on cyberviolence.[68] However, research is increasing, with a focus on cyberviolence, as the manifestations of this problem spread.

One significant source of data and information about cyberviolence is posted online by the Canadian Women's Foundation.[69] It is recommended that readers of this report access and scroll through the various chapters of this website.

Some of the witnesses who testified before the Canadian Parliamentary Committee that examined violence against young women and girls provided the following data:

- In 2014, 6 per cent of Canadians 15 years of age and over who use the Internet had been victims of cyberbullying in the past five years.
- The most common cyber offence against female children and youth is child luring, followed by invitation to sexual touching.
- Over 4,000 child sexual exploitation offences were reported in 2014, a 6 per cent increase over 2013.
- A January 2016 report revealed that of 44,000 images of child sexual abuse examined, 80 per cent of the children in the images were female. In addition, 79 per cent of them appeared to be prepubescent (under 12 years of age) and of that number, around 65 per cent were under eight years of age.
- In images of child sexual abuse, the perpetrators are disproportionately male; in one study, 83 per cent of images had a male perpetrator visible.
- The Canadian Centre for Child Protection receives around 15 reports a month dealing with online extortion of youth, although this figure is the 'tip of the iceberg'. The majority of these reports involve female child victims (70 per cent).[70]

Regarding exploitation of youth, Public Safety Canada reported in 2021 that:

- Over 4.3 million child sexual exploitation reports were processed by Cybertip.ca (i.e., a national tip line) from 2014 to 2020.
- There has been an 88 per cent increase in the reporting of sextortion and other online exploitation of youth since the COVID-19 pandemic began.
- Nearly one in four parents have come across inappropriate behaviour online aimed at their child.
- Thirty-nine per cent of luring attempts reported to Cybertip.ca in the last two years involved victims 13 or under.[71]

A report by Statistics Canada found that '17% of the population aged 15 to 29 (representing about 1.1 million people) that accessed the Internet at some point between 2009 and 2014 reported they had experienced cyberbullying or cyberstalking'.[72] The report also indicated that young women were more likely to 'have experienced both cyberbullying and cyberstalking in the last five years'.[73] Statistics Canada also reported that single and separated/divorced women are more likely to report being cyberstalked.[74]

Research supported by the United Nations Children's Fund (UNICEF) indicated that, in Jamaica, almost 40 per cent of high school students have been contacted online, by persons unknown to them, 'in a way that made them feel scared or uncomfortable',[75] and '43% received messages online that were clearly inappropriate'.[76]

Jamaican media referred to research, which indicated that 'for every 10 people bullied, three will self-harm, one will have a failed suicide attempt, and one will develop an eating disorder. Many teens get depressed, entertain suicidal thoughts, and suffer from anxiety, self-esteem and other social issues stemming from bullying.'[77] The United Nations Educational, Scientific and Cultural Organization (UNESCO) found that one in three students between the ages of 13 and 15 has been harassed in Latin America and the Caribbean. While the most common

forms are physical or sexual, cyberbullying 'is one of the less usual types of bullying, but is constantly growing, which generates a lot of concern'.[78]

A study by the LEAF found that cyberviolence has a disproportionate impact on women and girls:

> [Cyberviolence] is a gendered phenomenon that disproportionately impacts women and girls, reflecting and perpetuating their inequality in society beyond and prior to the existence of the Internet. Research by the eQuality Project found that out of 114 Canadian criminal law decisions in 2017 that involved technology-facilitated violence, 90 identified the victim as a woman or girl, and 106 involved a male defendant. A 2018 survey on gender-based violence and unwanted sexual behaviour in Canada found that women were more likely than men to have 'experienced an unwanted behaviour that made them feel unsafe or uncomfortable in a virtual space in the past 12 months', and to have been 'pressured to send, share, or post sexually suggestive or explicit images or messages'. In addition, young women were 'twice as likely as their male counterparts to say someone on a dating site or app has called them an offensive name (44% vs. 23%) or threatened to physically harm them (19% vs. 9%).'[79]

A research study in Trinidad and Tobago also found that females were at higher risk of being victims to both unauthorised access and cyberbullying incidents than were males (54.3 per cent female; 45.7 per cent male), with a higher proportion of both females and males being subject to unauthorised access crime than cyberbullying (34.1 per cent of respondents were victims of unauthorised access, and 18.1 per cent were cyberbullied). Younger age groups also had a higher probability of being harassed.[80] The researchers concluded that target exposure and accessibility (i.e., amount of time spent in online activities) increases the risk of victimisation, and does so more for cyberbullying.[81] The research also noted that victimisation rates appear to be lower in Trinidad and Tobago than in North America and Europe.[82] The researchers suggest that the type of online activity in which victims/survivors engage is a determining factor and that 'education on online activities and behaviour may be more prudent in cybercrime prevention'.[83]

However, research by UNICEF in the Eastern Caribbean Area (ECA)[84] revealed a more mixed pattern across the ECA as between males and females. However, the study included all forms of bullying (physical and verbal, and cyberbullying), and other Caribbean research by UNESCO indicates that physical and sexual bullying are the most common forms (cyberbullying less so), and males may be at greater risk of suffering from physical bullying while girls suffer more cyberbullying.[85] This may be supportable in the UNICEF study's data regarding the ECA, because 25 per cent of children (aged 13–15 years) had been harassed, and 38.5 per cent had been involved in physical fights (which likely indicates male victims). In the ECA, 25 per cent of secondary school children experienced bullying at least one day within the past month of the study.[86]

The preliminary results of research in Barbados revealed that about 20 per cent of respondents had been a victim of online abuse, and 65 per cent reported receiving nude or semi-nude photos that they believed were intended to be private. While most respondents (82 per cent) indicated that they never shared nude or semi-nude photos, 17 per cent admitted to having shared them in the past. Women appeared disproportionately affected, with 49 per cent of respondents indicating that a woman was the subject of the most recent photo they received.[87]

Regarding cyberviolence in intimate partner and dating relationships, a national survey in 2017 of transition and women's shelters in Canada revealed that:

> respondents reported 18 forms of technology-enabled abuse among those who sought help at their organizations, including (rounded to nearest whole number): sending threats and intimidating messages (93%); tracking the person's location through their phone, GPS, or another location service (66%); impersonating the person through their email or online profiles (62%); hacking into social media, email, or utilities accounts (62%); monitoring online activities and exfiltrating data (43%); tracking or monitoring the woman through devices that the abuser gave to their children as gifts (28%); and installing spyware or keyloggers (21%).[88]

2.2 Court Cases

LEAF also analysed and summarised several judicial decisions. The following provides a few excerpts from their analysis:[89]

> Speech-based TFGBV[90] through digital platforms, which have been documented in Canadian case law, includes behaviours such as:

- sending onslaughts of messages to women through social media platforms such as Facebook or other communications channels (including Twitter, email, voice, and text messages, and in at least one case, Google Review), despite their requests to stop and despite their taking actions such as blocking or deleting the harasser; (R v Broydell, 2018 CanLII 1161 (NL PC); R v Donatucci, 2009 ONCJ 734.)
- escalating volume, frequency, violence, and vitriol in communications in the absence of a response or if given a negative response (R v Broydell, 2018 CanLII 1161 (NL PC); R v Donatucci, 2009 ONCJ 734.); and
- creating and sending to the victim's co-workers a website with intimate details. (0 R v Fox, 2017 BCSC 2361, summarized in eQuality Project, "Technology-Facilitated Violence: Criminal Harassment Case Law" (3 July 2020), at 23, online (pdf): eQuality Project http://www.equalityproject.ca/wp-content/uploads/2020/07/TFVAWCriminal-Harassment-3-July-2020.pdf)

Threats to women have also extended to their family members. In at least one documented case, an individual posted to Facebook 'a threat to cause death or bodily harm to All Women' (R c Hunt, 2012 QCCA 4688).

Women are additionally affected by expression that attacks them based on intersecting marginalised identities. For example, one case involved someone posting threats and hateful language with respect to Muslim individuals. (R c Rioux, 2016 QCCQ 6762.)

In *R v. Fox*, the perpetrator 'sent [the targeted individual] hundreds, if not thousands, of emails to her and people she knew with the intention of degrading, humiliating, and tormenting her'. The emails included comments such as 'I will destroy you – slowly and incrementally [...] Every moment of my life is focused on the single goal' (summarized in eQuality Project, "Technology-Facilitated Violence: Criminal Harassment Case Law" (3 July 2020), p. 23, available at http://www.equalityproject.ca/wp-content/uploads/2020/07/TFVAW-Criminal-Harassment-3-July-2020.pdf). Other cases involved setting up a fake Facebook profile to catfish a former spouse to fraudulently extract information from her (R v Smith, 2014 ONCA 324, summarized in eQuality Project, "Technology-Facilitated Violence: Criminal Harassment Case Law" (3 July 2020), at 67, available at http://www.equalityproject.ca/wp-content/uploads/2020/07/TFVAWCriminal-Harassment-3-July-2020); and sending a classmate unwanted Facebook messages describing violent sexual fantasies involving her (R v DD, 2013 ONCJ 134).

Often the abusive expression is combined with other forms of violence, abuse, or harassment that exceed the boundaries of speech-based TFGBV to overlap with other substantive harms such as invasion of privacy, violation of sexual boundaries, impersonation, defamation, and putting the victim in physical danger in addition to psychological distress. This has included harassing the victim in person or through sending physical mail and unwanted objects; distributing nude photos of the victim to the public and to the woman's co-workers, family, and friends (R v Wenc, 2009 ABCA 328; R v SB et al, 2014 BCPC 279; and R v Korbut, 2012 ONCJ 691.); creating fake social media profiles impersonating the victim and making false claims (e.g., that the victim was spreading HIV) (R v Wenc, 2009 ABCA 328; R v SB et al, 2014 BCPC 279; and R v Korbut, 2012 ONCJ 691.); impersonating the victim to set up sexual encounters with male strangers online and sending them to the victim's apartment for sex, without her knowledge (R v Korbut, 2012 ONCJ 691, summarized in eQuality Project, "Technology-Facilitated Violence: Criminal Harassment Case Law" (3 July 2020), at 68, available at http://www.equalityproject.ca/wpcontent/uploads/2020/07/TFVAW-Criminal-Harassment-3-July-2020.pdf); recording the victim engaged in sexual activity without her knowledge or consent, and distributing the video on Facebook and through email to her friends and family (R v PD, 2011 ONCJ 133) hiding an Internet-connected webcam in her bedroom; (R v Corby, 2016 BCCA 76.); doxing and SWATTing her (R v BLA, 2015 BCPC 20) sextortion; (R v MR, 2017 ONCJ 943, summarized in eQuality Project, "Technology-Facilitated Violence: Criminal Harassment Case Law" (3 July 2020), at 56-57, available at http://www.equalityproject.ca/wpcontent/uploads/2020/07/TFVAW-Criminal-Harassment-3-July-202); taking over the victim's own social media accounts (R v

MR, 2017 ONCJ 943); covert surveillance and tracking and monitoring the victim through her digital devices (R v Smith, 2014 ONCA 324.); sexual luring and child sex exploitation (R v Adams, 2016 ABQB 648); and non-technological forms of violence and abuse, such as stalking, in-person harassment, assault, and sexual assault (R v CL, 2014 NSPC 79.).

In one case with a particularly reprehensible and wide-ranging suite of abusive behaviours, involving at least 25 known victims, 'Mr. B used a variety of tactics to harass, threaten, and harm his victims, many of whom were female video gamers he encountered online [often through the livestreaming platform Twitch.tv]'. (9 R v BLA, 2015 BCPC 203, summarized in eQuality Project, "Technology-Facilitated Violence: Criminal Harassment Case Law" (3 July 2020), at 31-32, available at http://www.equalityproject.ca/wpcontent/uploads/2020/07/TFVAW-Criminal-Harassment-3-July-2020.pdf)

Women are also abused and harassed on digital platforms in response to and in direct relation to their professional activities and political views. As Sundén & Paasonen note, 'Online misogyny violently targets non-men, non-white, and non-straight subjects who make noise and embody difference on public online platforms. Public figures like politicians and journalists inhabit particularly vulnerable positions, as do authors, artists, and musicians who stand up for feminism and anti-racism.' (Jenny Sundén & Susanna Paasonen, "Shameless hags and tolerance whores: feminist resistance and the affective circuits of online hate" (2018) 18:4 Feminist Media Studies 643 at 650.)

A comprehensive analysis of prosecutions in the Caribbean is not readily available. However, there exists several media reports. For example, Jamaican media noted a conviction for a significant case of cyberbullying involving sextortion, where for several months a 30-year-old perpetrator displayed pornographic photographs and videos of individuals with the intent to extort money in exchange for the removal of the photographs or videos.[91]

These actual prosecutions are reflective of the various forms of cyberviolence described in Section 1.2 and, in particular, display the violent, coercive, controlling, racist and misogynistic nature of the perpetrator's motivation and harm.

3 Impact of Cyberviolence

Although broader in its scope than just the Commonwealth members, the Special Representative of the UN Secretary-General on Violence against Children has produced a report that outlines in detail the impact of cyberbullying on children across the world, which is worth considering.[92] The present report, however, will limit itself to findings among sources in the Caribbean and Americas region of the Commonwealth, which significantly confirm the findings of the UN report.

Cyberviolence has a disproportionate impact on women and girls in particular, where there is also intersectionality of race, ethnicity, religion, sexual orientation, poverty, disability and other socio-economic factors that marginalise them. The following summarises some of the various negative impacts that cyberviolence has wrought on women and girls.

Loss of reputation and other resulting consequences from cyberviolence has psychological, physical and socio-economic impacts. It can lead to social withdrawal, physical and psychological illness and low self-esteem, and cause ill effects on their familial, social and employment relationships, sexual and psychological integrity, autonomy, equality and privacy. It can also 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, cyberviolence can lead women and girls to commit suicide'[93] – as it did in the case of Rehtaeh Parsons in Nova Scotia and Amanda Todd in British Columbia.[94]

One Canadian survey of 60 respondents concluded that cyberviolence has a major impact on women's mental health, safety and well-being, noting the following ill effects: anxiety (48 per cent), damaged self-image (43 per cent), withdrawal from online activity (40 per cent), shame and humiliation (30 per cent), isolation from friends and family (28 per cent), job impact (13 per cent), suicidal or self-harm thoughts (10 per cent).[95] Women who experienced cyberstalking were 25 per cent less likely than other women to rate their mental health as good or excellent, and reported being less satisfied with their personal safety as compared to males who had been cyberstalked (75 per cent as opposed to 87 per cent).[96] A survey of secondary school students found that girls who had experienced cyberbullying

were twice as likely as boys to feel stressed, hopeless and overwhelmed.[97] Also, girls have been found to be more prone to suicidal thoughts/attempts than boys.[98]

Similar impacts have been noted in the Caribbean, with cyberbullying being a new form of aggression, humiliation and intimidation by anonymous people, resulting in social violence in both online and offline communities. A 2018 study found that 'Caribbean people are prone to online rape of their identity, experience on social media manipulation and calumny of their reputation and succumbed to physical and psychological abuse'.[99] This experience humiliates their private life, identity and self-esteem, in both online and offline realities, influences mental and social relationships and can even endanger their physical security. The same study posits that in some Caribbean communities, victims of cyberbullying are sometimes physically attacked by community members and strangers.[100]

The two prominent cases of suicide that occurred in Canada, noted above, are evidence that what occurs online can have significant consequences in the real world, and that 'the distinction between cyberspace and real space is virtually meaningless'.[101]

Use of social media by the youth is an intrinsic part of their lives, and they use it as their main means of communication. What happens in cyberspace is also carried through to the physical world, such that both are considered real space for them. The two cases are also significant because they demonstrate the acceleration and accentuation effect that online bystanders can play in furthering the harms of cyberviolence.

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. While 89 per cent of teachers in a Canadian study considered bullying to be a serious problem, and 71 per cent said they usually intervened with bullying problems, only 25 per cent of students said that their teachers intervened.[102]

A study in Trinidad and Tobago of university students examined 'the link between social bonds in the form of peer and intimate partner relationships resulting in feelings of anger, depression, low self-esteem and suicide ideation and the increased likelihood of persons engaging in cyberbullying or becoming victims of cyberbullying'.[103] The study found that self-reports by students of having engaged in cyberbullying (88.5 per cent) outnumbered the self-reports of victimisation (28.5 per cent). While social-psychological constructs (such as self-esteem, suicide ideation and depression) influenced those who engaged in cyberbullying behaviours, the key influencer was found to be anger. While social bonds with other peers also played an integral role (i.e., the theory being that persons with low social bonds to peers or intimate partners would be more likely to engage in cyberbullying or become cyber-victims, and vice versa those with strong social bonds would be less likely), social bonds were not enough to deter university students from engaging in cyberbullying.[104]

Some studies suggest that cyberviolence negatively effects women's and girls' public and democratic participation in society and can relegate them to secondary status both online and in society in general:

> They are rendered unable to freely and fully participate in society and prevented from enjoying true or equal protection of their human rights and fundamental freedoms, including the right to freedom of expression. The most common response to facing online abuse and harassment is that women reduce their online activities, avoid certain social media platforms or conversations, withdraw from expressing their views, or self-censor if they continue to engage online. In other words, women are 'driven off of the Internet'. This curtails their ability to participate in the contemporary public sphere, including engaging in activism and advocacy, influencing public opinion, or mobilizing social, cultural, or political change.[105]

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 due to their public presence and the exercise of their freedom of expression:

> According to a 2016 Inter-Parliamentary Union study, 82 per cent of female parliamentarians in 39 countries across five global regions have experienced some form of psychological violence (remarks, gestures and images of a sexist or humiliating sexual nature made against them or threats and/or mobbing) while serving their terms. They cited social media as the main channel through which such psychological violence is perpetrated; nearly half of those

surveyed (44 per cent) reported having received death, rape, assault or abduction threats towards them or their families.[106]

As further evidence that cyberviolence can also mirror or influence conduct in the physical world, the same survey noted that 65 per cent of these female politicians 'had been subjected to sexist remarks, primarily by male colleagues in parliament and from opposing parties as well as their own'.[107]

Female journalists and feminist activists are also particularly targeted for their exercise of free speech and expression. A study by the UK-based *Guardian* newspaper noted that a significantly higher proportion of commentary by female journalists was blocked by moderators due to supposed violations of commenting policy, and that 57 per cent of abusive comments targeted at them 'focused on their body, private life, or sexuality', over three times more than similar comments aimed at male journalists.[108]

Misogynistic and sexist expression on social media has also been evidenced in professional schools, such as law and medicine, and in the arena of pop culture.[109]

Doubly concerning is that 'women are not only targeted online for writing, speaking, engaging in politics, advocating for substantive equality, or making their way in professional or male-dominated spaces, but also for attempts to hold the perpetrators of this very abuse accountable'.[110]

The harmful consequences and impact of cyberviolence are 'further layered and experienced in unique and additionally devastating ways by women and girls with other intersecting identities that also face systemic discrimination'.[111] The impact is further exacerbated where the individuals belong to more than one historically marginalised group, characterised by race, ethnicity, indigenous heritage, religion, mental or physical disability, immigrant or refugee status, sexual orientation, etc. For example, a 2011 Canadian study found that students belonging to sexual orientations other than the heterosexual orientation were more likely to be targets of online bullying, harassment and hate.[112] 'While 5.7% of heterosexual students were targeted online, 30% of female sexual minority students, 40% of transgender students, and 23% of gay male students said they were targeted.'[113]

Again, the consequences of the cyberviolence are mirrored and experienced in the physical world. 'For example, Inuit women in Nunavut face criminal harassment, sexual assault, and "indecent or harassing communication" at 3.6 times, 7.2 times, and 8.9 times the Canadian national average, respectively. This disproportionate impact is reflected in online abuse targeting them as well.'[114]

Concern has also been expressed in the Caribbean about incidents of cyberbullying that focused on the sexual orientation of the targeted person, and which subsequently led to physical assaults and death.[115]

Lastly, 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.

4 Perpetrators vs. Bystanders

In examining the phenomenon of cyberviolence, one must distinguish between perpetrators, bystanders and victims/survivors, especially within the context of peer group and intimate partner relationships where interpersonal relations and emotions can be complex.

In a general and non-legal sense, a perpetrator is any individual who intentionally and knowingly commits cyberviolence. However, as discussed in Section 5, online bystanders may, depending on the circumstances and their level of awareness, also be equally liable under the criminal law as being aiders and abettors to the perpetrator's crime, or even be co-perpetrators. Even 'innocent' bystanders may unwittingly, or be misled to, contribute to the cyberviolence.

As noted in earlier sections of this report dealing with forms of cyberviolence and its impacts, some forms of cyberviolence are accentuated and accelerated due to further distribution of harmful content by co-perpetrators or bystanders. This may involve a single perpetrator or 'a small group of actors who planned and coordinated the mobbing, with other individuals joining in either knowingly, recklessly or being misled into piling in without awareness of the full context'.[116] Thus, viewers of online content (or bystanders) may be recruited, or act on their own accord, to deliberately further the cyberviolence, or unwittingly or be misled to further distribute the communication without full awareness of the harmful context or harmful impact. 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. Some persons are clearly culpable, while others are

recruited or duped to participate in the distribution and harmful consequences or are oblivious to or reckless regarding the context or implications of what they are doing as they consider it as simply humorous or normal conduct.

The Canadian Parliamentary Committee studying online violence heard evidence of 'one study in which 65% of young people between the ages of 9 and 17 years said they would engage in the non-consensual distribution of intimate images and sexting for fun or to make friends laugh'.[117] The Committee also heard a number of witnesses who spoke to the current online culture among youth where 'online violence has become normalized, with many youth believing that cyberviolence is an inevitable component of Internet and mobile device use', and that such violence 'in turn makes violence in off-line environments more acceptable'.[118]

A similar culture was noted in the Caribbean region where bullying (according to some authors) is not taken seriously by stakeholders in the education and public health sectors or by policy-makers, and 'some people trivialized bullying as normal group activity'.[119] Preliminary results of a survey in Barbados indicated that 65 per cent of respondents reported receiving nude or semi-nude photos that they believed were intended to be private. While most respondents (82 per cent) indicated that they never shared nude or semi-nude photos, 17 per cent admitted to having shared in the past.[120]

Social and psychological research has examined the dynamics of bystander behaviour and its impact on victims/survivors. It has been postulated that victims may experience more harm from cyberbullying than face-to-face bullying, because the online nature increases the likelihood of negative bystander behaviour, that is, distributing the content to other audiences and media sites.[121] It is essential to understand the ways in which bystanders respond to cyberviolence, and their motivations, because bystanders can be either 'negative bystanders', who encourage or further the commission of the cyberviolence, or 'positive bystanders', who intervene and defend the victim/survivor.[122]

Another form of bystanders are social media platforms on and through which cyberviolence is committed. Some platforms claim to be merely common carriers with no responsibility for the content that passes through their systems. However, some authors posit that in some circumstances they could and should be held criminally or civilly liable.[123] This is discussed later in this report.

5 Current Legal Framework

This section examines the current legal framework and how some online bystanders may be 'negative bystanders', and even be subject to criminal or civil liability. Later in this report, we examine measures to encourage bystanders to be 'positive bystanders'.

5.1 Criminal Law

This section generally follows the classification of 'Types and Modes of Cyberviolence' discussed earlier in this report and examines how current criminal laws may hold perpetrators and bystanders legally accountable. For the purpose of analysis, specific reference is made to some Canadian and Caribbean criminal laws, but many of these laws are equally reflective of common law principles or statutory offences applicable in many Caribbean jurisdictions. The examples considered are used as an analytical framework from which other jurisdictions can compare their own criminal laws.

Jurisdictions that have a criminal code or penal code, or other statutory consolidation of laws, generally contain a provision that outlines the various modes of participation in the commission of an offence. For example, subsection 21(1) of the Criminal Code of Canada provides:[124]

> 21(1) Everyone is a party to an offence who
>
> a. actually commits it;
>
> b. does or omits to do anything for the purpose of aiding any person to commit it; or
>
> c. abets any person in committing it.

Those who aid or abet a direct perpetrator of an offence are regarded as being equally liable for its commission, just as is the actual perpetrator. With respect to paragraph (a), the perpetrator or principal may act alone, or jointly with another co-perpetrator or co-principal. Paragraph (b) holds individuals to be equally liable as parties if they knowingly/intentionally do or omit to do anything for the purpose of aiding another person (a principal) to commit the offence. Paragraph (c) includes various situations where a person intentionally encourages, by acts or words, the commission of the offence by another person, or intentionally prevents or hinders an interference with the accomplishment of the criminal conduct.[125]

Subsection 21(2) imposes liability for persons acting together in joint ventures, and attaches

liability (as a party) for what may be considered as collateral crimes committed by one or more of the joint venturers carrying out an unlawful purpose, if the causing of the collateral crime is known to be a probable consequence of carrying out the common purpose.[126] Subsection 22 provides that persons who intentionally encourage, incite, solicit or procure another person to commit an offence are also considered to be parties to that offence if committed. Where the offence counselled (incited) is not committed, s. 464 provides that the person who counselled its commission may be liable for a separate offence.

Clearly, depending on the circumstances, the person's conduct and their level of awareness (i.e., intent, knowledge), 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, or an inciter or procurer.

Likewise, The Bahamas has a statutory provision in its penal code that addresses various modes of participation in a criminal offence. Section 86 provides:

> Whoever directly or indirectly, instigates, commands, counsels, procures, solicits or in any manner purposely aids, facilitates, encourages or promotes, whether by his act or presence or otherwise, and every person who does any act for the purpose of aiding, facilitating, encouraging or promoting the commission of an offence by any other person, whether known or unknown, certain or uncertain, is guilty of abetting that offence, and of abetting the other person in respect of that offence.[127]

Persons who are guilty of abetting are equally liable as is the principal perpetrator.[128] Therefore, bystanders could be criminally liable if their conduct and mental state meets the requirements of this statutory provision.

Some jurisdictions have specifically included provisions in their cybercrime statutes to address participation in the commission of an offence, including such conduct as incites, counsels, solicits, procures, facilitates, aids and abets, and either provide that the person is subject to a specific penalty or is equally liable as the principal offender.[129]

Jurisdictions that do not have statutory provisions on modes of participation in an offence rely on common law principles and jurisprudence, which may also make bystanders criminally liable as co-perpetrators or as aiders or abettors.

The above criminal law principles, regarding modes of commission of an offence, are applied to the various types of cyberviolence discussed earlier and to the applicable domestic criminal law offences within the Americas region of the Commonwealth being studied here.

5.1.1 Cyber-harassment

Various criminal offences may be applicable. In Canada, the general offence of harassment is the most common offence that can address situations of 'cyberbullying'. The offence consists of intentional repetitive conduct or communications to another person, including threats, that in the circumstances reasonably causes that person to fear for their safety or the safety of another person known to them, if the offender knows or is reckless (i.e., has reckless disregard) as to whether that person is harassed.[130] The offence of harassment is technologically neutral and applies equally to both the online and offline realms.

In jurisdictions which encompass mental elements (*mens rea*) of intent, knowledge or recklessness in the definition of an offence, and depending on the circumstances, bystanders could be equally liable as perpetrators.

Canada also has specific types of harassment offences involving sending telecommunications to another person, such as sending false messages with intent to injure or alarm, sending indecent messages with intent to alarm or annoy, or repeatedly communicating with intent to harass.[131] There is also an offence of making, publishing, distributing or circulating obscene materials (in any form), and possession of such materials for the purpose of publication, distribution or circulation. The offence is technologically neutral and applies equally to both the online and offline realms.[132] Again, persons who aid or abet, or incite, the commission of these offences may also be held criminally liable.

The non-consensual distribution of intimate images could constitute the criminal offence of harassment, if requisite elements of the offence, as noted above, are met.

Canada has specifically criminalised the non-consensual distribution of intimate images. A person who 'knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct' is guilty of this offence. The definition of 'intimate images' includes photographs, film or video recordings of a person's nudity, exposure of genital organs, anal region or female breasts, or engagement in explicit sexual activity, where at the time of the recording the circumstances give rise to a reasonable expectation of privacy, and at the time of the publication/distribution the person depicted retains a reasonable expectation of privacy.[133] Further provisions permit a court to order: removal of non-consensual images from the Internet; forfeiture of a computer, cell phone or other device used in the commission of the offence; prohibition of the use of the Internet as part of the offender's sentence; reimbursement to victims for costs incurred to remove the intimate images; and prevention of a person from distributing the intimate image.[134]

A separate offence also exists in Canada of voyeurism, which penalises a person who surreptitiously observes or makes a visual recording of a person who is nude, exposes their genital or anal regions, or is engaged in sexual activity, in circumstances that give rise to a reasonable expectation of privacy.[135] The offences of voyeurism and distribution of intimate images are technologically neutral, and apply equally in the offline and online realms.

Antigua and Barbuda, and Grenada, enacted a cyber offence of violation of privacy that criminalises any person who 'intentionally and without lawful excuse or justification captures, publishes or transmits the image of the private area of another person without his or her consent', under circumstances violating the privacy of that person. 'Capture' means to 'videotape, photograph, film, or record by any means', and 'private area' means 'the naked or undergarment clad genitals, pubic area or buttocks of a person, or female breast'.[136]

St Vincent and the Grenadines has a law that creates the offence of violation of privacy. It criminalises a person who, intentionally and without lawful excuse, captures, stores, publishes or transmits through a computer system the image of a private area of a person without consent, where there is a reasonable expectation of privacy to disrobe or not be visible to the public whether in a public or private place. There is also an offence of sexual harassment by electronic communications that addresses the distribution, by computer systems, of sexually explicit images of a person that conveys or contains the personal identification information of the person.[137]

Guyana has a violation of privacy offence which is similar to that of St Vincent and the Grenadines, with a mental element of intent and lack of consent of the person depicted, but without a requirement of a reasonable expectation of privacy. It also has provisions providing for forfeiture and compensation.[138] Belize also enacted an offence of publication/transmission of private images, which is similar to that of Guyana in terms of mental and physical elements, and has a forfeiture provision, as well as an order to prohibit an offender to use the internet/computer system.[139] These offences would address cyberviolence in the form of voyeurism and non-consensual distribution of intimate images.

St Vincent and the Grenadines' legislation also contains a specific offence of cyberbullying. It criminalises a person who, intentionally or recklessly, uses a computer system, repeatedly or continuously, to distribute or transmit a communication, statement or image that causes a person to feel frightened, intimidated or distressed, or causes harm to that person's health or reputation.[140] It also enacted an offence of harassment by electronic means to criminalise a person who, intentionally or recklessly, uses a computer system to send another person any information, statement or image that is obscene or constitutes a threat or is menacing in character, and thereby causes the other person to feel intimidated, harassed or threatened.[141] The Act also contains procedural provisions to permit restraint and removal and forfeiture of the material. Due to the vagueness of some of the language and concerns about freedom of speech and expression, the Act has been strongly criticised.[142]

Barbados and Jamaica have a similar offence of malicious communication that penalises a person who uses a computer to send data that is obscene, constitutes a threat or is menacing in character or nature, and who intends or is reckless in whether

such conduct 'causes annoyance, inconvenience, distress or anxiety' to any person.[143]

St Kitts and Nevis also has a similar offence addressing the sending of obscene, threatening or menacing computer communications, but requires intent to cause a person 'to feel intimidated, molested, harassed or threatened'.[144]

Saint Lucia and Grenada's law on cyberstalking provides that a person shall not 'intimidate, coerce, insult or annoy another person using an electronic system'.[145]

Antigua and Barbuda have a law criminalising electronic harassment or intimidation. It criminalises persons who 'intentionally, without lawful excuse or justification, intimidate, coerce or harass another person using an electronic system'.[146]

Grenada, and Antigua and Barbuda, have also enacted offences to prohibit the sending of offensive or threatening messages through communication services.[147] However, following criticism about the laws' vagueness of language and impact on freedom of expression, both Grenada, and Antigua and Barbuda, amended/repealed some of these provisions. For example, Antigua and Barbuda's amended law only applies to threatening messages ('offensive' has been deleted), and also repealed a provision dealing with the causing of 'annoyance or inconvenience'. Grenada repealed its offences of sending offensive/threatening messages and electronic stalking.[148]

Guyana and Belize, respectively, enacted several laws criminalising the use of a computer to coerce, harass, intimidate or humiliate another person. These include intimidating a person or threatening a person or their family with violence, or threatening damage to property, with intent to compel that person to do or refrain from doing any act which the person has a legal right to do; publishing/transmitting computer data that is 'obscene, vulgar, profane, lewd, lascivious or indecent with intent to humiliate, harass or cause substantial emotional distress to another person'; or repeatedly send such data 'to the detriment of that person's health, emotional well-being, self-esteem or reputation'.

Guyana and Belize also both enacted a computer defamation offence which addresses the causing of damage to a person's reputation or subjects the person 'to ridicule, contempt, hatred or embarrassment', as well as an offence of computer extortion by threatening to publish personal/private information that can cause 'public ridicule, contempt, hatred or embarrassment'.[149]

British Virgin Islands (UK overseas territory) also enacted a new law that criminalises the distribution of intimate images and sending of 'offensive' or 'menacing' messages for the purpose of 'causing annoyance or inconvenience', as well as an electronic defamation law.[150] Despite being heavily criticised in the media, the new law was eventually given assent and brought into effect.[151]

These offences in the Caribbean region, discussed above, would address various forms of cyberbullying, cyber-harassment and distribution of intimate images, as well as defamation in some circumstances.

Trinidad has proposed the enactment of new computer-related offences to criminalise cyberbullying/harassment and the non-consensual distribution of private images, which is discussed in Section 9.[152]

Depending on the circumstances, in particular whether the bystander had knowledge/intent or recklessness as to whether the depicted person did not give their consent to the distribution of their intimate image, or the bystander had intention or recklessness as to the causing of harmful consequences flowing from forwarding the communications to others, a bystander could be held equally liable as is a perpetrator or co-perpetrator of these offences of distribution of intimate images and cyberbullying/harassment. Likewise, bystanders could also equally be criminally liable if they aid or abet the commission of the offence by a perpetrator or co-perpetrator.

St Kitts and Nevis has a specific offence addressing the republication of an obscene, threatening or menacing electronic communication to other persons (other than the person who is the subject of the message), without lawful excuse or justification.[153]

A number of Caribbean Commonwealth jurisdictions have various criminal laws that restrict freedom of expression where such expression may harm a person's reputation, such as criminal defamation and libel laws.[154]

As noted above, Antigua and Barbuda, Barbados, Belize, Grenada, Guyana, Jamaica, Saint Lucia, St

Vincent and the Grenadines, and the British Virgin Islands specifically enacted laws that either refer to electronic defamation or sending offensive or menacing messages (i.e., messages which can be interpreted as defamation) by electronic means of communication. Due to criticisms, some of these laws have subsequently been amended, while others have not.[155]

While the criminal laws addressing defamation in other jurisdictions are of general application, they do not appear to distinguish between various media of publication, and, thus, could apply to Internet and mobile phone communications that damage a person's reputation or expose the person to hatred, contempt or ridicule.[156] Canada also has criminal laws addressing defamatory libel,[157] but some courts have declared some of the provisions to be unconstitutional.[158]

Many of the new laws in the Caribbean jurisdictions are limited to communications made through computer or electronic systems, which limits their scope of application to online environments, and may not capture other means of communication by telecommunication (e.g., telephone) or orally in person (offline). British Virgin Islands amended its computer crime law to extend its application to telephone mobile networks.[159] This issue is discussed further in Section 9.1.

5.1.2 ICT-Related Violations of Privacy

Various criminal offences may be applicable to address the various types of conduct involved in cyberstalking. The Canadian criminal offence of uttering threats to cause death or bodily harm, or to harm or destroy real or personal property, may be applicable in both the offline and online realms.[160] Some jurisdictions, such as Canada, Guyana and Belize, have specific offences to address intimidation of a person by threats of violence for the purpose of compelling them to abstain from doing something that they have a right to do, or to do anything they have a right to abstain from doing.[161] As noted above, a number of Caribbean jurisdictions, such as Antigua and Barbuda, Grenada, Saint Lucia and St Vincent and the Grenadines, have enacted specific electronic harassment, intimidation and stalking offences, which include the making of threats.

Where interception of private communications or data is involved in the cyberviolence, various criminal offences may be applicable, such as: offences against the interception of oral or telecommunication interactions;[162] or specific computer crime offences involving the unauthorised use of a computer system, obtaining of computer system services or interception of computer system functions.[163] These offences could address directly some forms of cyberviolence that involve violations of privacy, as well as criminalise the unauthorised access or obtaining of personal data from computer systems, which can subsequently be used to commit other types of cyberviolence such as intimidation, doxing, impersonation and sextortion.

Cyberviolence involving voyeurism (i.e., surreptitiously observing or recording a person who is in an intimate situation and within a circumstantial context that gives rise to a reasonable expectation of privacy) may be addressed by specific offences of voyeurism.[164] As noted above, a number of Caribbean jurisdictions, and Canada, have enacted violation of privacy offences that address voyeurism and the non-consensual capture and distribution of intimate images.

Cyberviolence involving the creation of fake social media accounts, manipulation of images or fraudulently impersonating another person may, depending on the circumstances, be addressed by offences against forgery,[165] fraud,[166] theft of identity information, trafficking in identity information or identity fraud.[167]

Cyberviolence involving sextortion may be addressed by traditional offences of extortion, because engaging in sexual activity or sending of intimate photos can constitute extortion.[168] Also, the offence of intimidation and computer extortion, discussed above, may also be applicable.[169]

Bystanders who aid or abet perpetrators in the commission of any of the above-noted criminal offences may, depending on the facts of each matter, also be held criminally liable.

5.1.3 Online Sexual Exploitation and Sexual Abuse

All jurisdictions in the Caribbean and Americas region of the Commonwealth have various offences addressing sexual exploitation and sexual abuse of children. Some jurisdictions have a more extensive range of offences than others.[170] Those jurisdictions that have enacted offences in accordance with the Commonwealth Model Law on Computer and

Computer Related Crime will have offences that align with this form of cyberviolence, as discussed above in Section 1.2.[171]

Jurisdictions that do not have specific cybercrime offences addressing child exploitation and sexual abuse may nevertheless be able to resort to their technologically neutral offences addressing similar conduct, such as procuring child prostitution, producing and distributing child pornography, corruption of children and luring or solicitation of children for sexual purposes.

At least one jurisdiction in the Commonwealth Americas and Caribbean region has a law requiring the mandatory reporting, by Internet service providers, of Internet child pornography.[172]

Bystanders who aid or abet perpetrators in the commission of any of the above-noted criminal offences may also be held criminally liable.

5.1.4 ICT-Related Hate Crime

Some jurisdictions, such as Canada, have specific hate crime offences, which criminalise the intentional promotion of hatred against an identifiable group, and which may include as defining characteristics of the identifiable group such characteristics as age, sex, sexual orientation and gender identity or expression.[173] These offences would address ICT hate-related cyberviolence against women and girls as an identifiable group, or of individuals within the group. Some general, criminal defamation and libel laws, as well as some computer intimidation laws, in the Caribbean may also criminalise exposing a particular person to hatred.[174]

Bystanders who aid or abet perpetrators in the commission of hate crimes may also be held criminally liable.

5.1.5 ICT-Related Direct Threats or Actual Violence

Some jurisdictions, such as Canada, have general (technologically neutral) offences that criminalise intentional threats to commit harm, such as sexual assault, assault and murder, including threats to harm the targeted person's family or friends.[175] As discussed earlier, some Caribbean jurisdictions' computer crime laws contain provisions that penalise the making of threats.

Regarding the cyberviolence activity known as 'SWATing', some jurisdictions have offences that threaten the integrity of the administration of justice, which may include intentionally and falsely accusing a person of having committed a crime, and reporting to the police that a crime has been committed when it has not. Such activity may cause the police to begin or continue an investigation when there is no basis for doing so.[176]

Bystanders who aid or abet perpetrators in the commission of any of the above-noted criminal offences may also be held criminally liable.

5.1.6 Cybercrime and other Cyber Manipulations

With respect to various forms of cyberviolence that incorporate the commission of cybercrimes, such as illegal access to personal data, manipulation or destruction of data, interference with access to data, unauthorised use of computer systems and interception of computer functions, those jurisdictions that have enacted offences in accordance with the Commonwealth Model Law on Computer and Computer Related Crime would have the necessary criminal offences to address forms of cyberviolence that employ these cybercrimes to commit or further the cyberviolence.[177] Manipulating computer data within ICT systems to create false messages or change algorithms, which determine what content is promoted or supressed, could fall within the purview of these cybercrimes.

Some Caribbean countries, such as Dominica, and other United Kingdom overseas territories, such as Anguilla, Montserrat and Turks and Caicos, either do not have computer crime/cybercrime laws, or are in the process of drafting such laws. The UK territories of Bermuda and Cayman Islands have computer misuse laws addressing only more traditional computer crime offences, such as unauthorised access, modification of data and interception or interference with computer functions/services.[178]

5.2 Civil Law

5.2.1 Common Law Torts

The most common tort to address cyberviolence that involves harm to one's reputation is the common law tort of defamation, which exists in all jurisdictions within the Commonwealth Caribbean and Americas region. This tort addresses the spreading of false information about a person, which harms their reputation. If the speech/communication is live and unrecorded, it is slander; if recorded, it is libel. Generally, to constitute

defamation, the statement must reasonably be considered to harm a person's reputation, be directed towards the plaintiff and be communicated to at least one other person.[179]

There has been significant litigation in Canada, including cases that have established new common law torts or have been adjudicated to the level of the Supreme Court of Canada, due to the important legal and public policy issues involved. This report will only note a few cases, which may be useful as precedent for other jurisdictions.

The case of *AB v. Bragg* dealt with defamation. The court obliged social media companies to divulge the identity of their account holder who had published the defamatory material. It also issued media publication bans and orders of anonymity.[180] In the case, a 15-year-old girl was targeted by a fake Facebook profile, created by an unknown person, that included her photo and a description of preferred sexual acts, appearance and weight. In the plaintiff's action for defamation, the provincial trial and appeal courts granted an order against Facebook to disclose the account holder's identity but denied the plaintiff's requests for anonymity and a publication ban. On appeal, the Supreme Court of Canada granted an order to give effect to the anonymity of the plaintiff's identity, but denied a complete publication ban against the media and permitted the publication of only non-identifying information about the girl.

Another landmark case is that of *Jane Doe 72511 v. NM*, which established a new common law tort of public disclosure of private facts.[181] In revenge for his intimate partner complaining to the police about several incidents of verbal and physical abuse, the male defendant posted a sexually explicit video of his intimate partner (woman plaintiff) on an internet pornography website (although the video was made with the consent of the women, its subsequent posting was not consensual), and then threatened to post further nude photos of the plaintiff if she proceeded with legal action against him. After reviewing other precedents and the legislative trend in this area, the trial judge held that a cause of action for 'public disclosure of private facts represents a constructive, incremental modification of existing law to address a challenge posed by new technology'.[182]

The case of *Caplan v. Atas* established a new common law tort of online harassment,[183] which would be applicable to many situations of cyberviolence. The tort addresses the causing of harm to the plaintiff as a result of the defendant's malicious or reckless making of communications that is outrageous in character, degree and duration and extreme in degree, so as to go beyond all possible bounds of decency and tolerance, and is made with the intent to cause fear, anxiety, emotional distress or impugn the dignity of the plaintiff.

Bystanders who redistribute the defamatory or other tortious communications could also be civilly liable as co-tortfeasors if their conduct meets the requisite standards of these tort laws.

5.2.2 Statutory Remedies

Six Canadian provinces – Nova Scotia, Saskatchewan, Manitoba, Alberta, Prince Edward Island, and Newfoundland and Labrador – enacted legislation that provides provincial offences and penalties[184] for the non-consensual distribution of intimate images and cyberbullying, as well as provide for the seeking of various statutory civil remedies.[185]

While the provincial statutes have differences in definition and scope, some of them generally provide for the ability, in respect of non-consensual distribution of images or cyberbullying, to make an application to a court in order to obtain judicial orders, and empower the court to make interim and final orders, such as:

- prohibiting a person from distributing the intimate image;
- prohibiting a person from contacting the applicant or another person;
- requiring that the applicant be given any information in the possession of a person that may help to identify a person who used an internet protocol address, website or electronic username or other unique identifier that may have been used to distribute an intimate image without consent or for cyberbullying;
- requiring a person to take down or disable access to an intimate image or cyberbullying communication;
- declaring that a communication is cyberbullying;
- referring the matter to a dispute resolution service;

- requiring a person to pay general, special, aggravated or punitive damages to the person depicted in the intimate image or the victim of cyberbullying;
- requiring a person to account for profits;
- giving effect to any order provided by regulations; and
- making any other order which is just and reasonable.[186]

Some statutes provide that various factors, if relevant, to be taken into account by a court in determining whether to make an order, such as: the content of the image or communication; the manner and repetition of the conduct; the nature and extent of the harm caused; the age and vulnerability of the person depicted in the intimate image or victim of cyberbullying; the conduct, and the purpose or intention, of the person responsible for the distribution of the image or the cyberbullying, including any efforts to minimise harm; the subject matter, circumstances and context of the conduct; the extent of the distribution of the intimate image or cyberbullying; the truth or falsity of the communication; and the age and maturity of the person responsible for distribution of the intimate image without consent or cyberbullying.[187]

A number of provincial and territorial legislatures have also enacted or amended various laws concerning education, placing obligations on schools and students in respect of bullying, including cyberbullying, such as bullying prevention, remedial programmes to assist victims, professional development for teachers about bullying and strategies to address it, and plans for positive learning environments free from harassment and bullying.[188] Some laws also require students to refrain from engaging in cyberbullying, to not tolerate it and to report it to school officials, subject to disciplinary sanctions for failure to abide by the law.[189] One province also makes parents responsible for their child's cyberbullying, if the parent was aware of it, could reasonably predict its effect and failed to stop it; as well as empower the courts to make protection orders.[190]

Several of the computer crime laws of Caribbean jurisdictions, as discussed earlier, have specific provisions relating to compensation and forfeiture in relation to the commission of their computer/cybercrime crime laws.[191]

6 The Role of ICT Companies/ Platforms

6.1 Liability of Digital Platforms

In Canada, there are a number of laws that could theoretically be used to establish civil or criminal liability for digital platforms. The Canadian LEAF report provides a comprehensive analysis of this issue.[192] Depending on the circumstances and involvement of ICT, laws that could apply include copyright laws (which provide notice and takedown), criminal laws addressing non-consensual distribution of intimate images, harassment or hate speech (depending on the level of knowledge and awareness of the ICT), statutory human rights laws, product liability laws and defamation law (where the ICT had specific knowledge 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 deindexing or disabling access to content.

St Vincent and the Grenadines has enacted comprehensive provisions addressing the liability and immunities of various types of internet service providers (regarding various activities/functions such as access, hosting, caching, hyperlinks and search engines). Essentially, these providers are not liable if they are not involved in any illegal activity or acts of interference, act expeditiously to preserve or remove data and comply with any court orders.[193]

Belize enacted a law to provide that a service provider or its users shall not be deemed as publishers or speakers of any information provided by another service provider or user.[194] This raises the question of whether Belize may have granted some form of immunity to bystanders as the provision appears to say that they are not deemed to be publishers or speakers of information provided by another user (e.g., the principal perpetrator) of the service provider. This is an issue that requires further reflection by Belize authorities. Belize also provides that a service provider shall not be liable for taking action to restrict access to material which is 'obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable'.[195]

6.2 ICT Measures to Address Cyberviolence

While various laws may apply to them, as discussed above, online platforms remain largely unregulated in Canada and the Caribbean. However, 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.[196] 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, and instead spread messages promoting equality, diversity, human rights and empathy.[197]

Witnesses before the two Canadian Parliamentary Committees (one examining cyberviolence, and the other examining online hate), including representatives of the ICT industry, stressed the need for government to establish clear rules regarding online hate and cyberviolence.[198] While it is important to hold ICT companies/platforms accountable, it 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.[199]

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

7 Challenges in Addressing Cyberviolence

The Council of Europe's report[200] highlighted several challenges to the investigation and prosecution of cyberviolence crimes. These considerations are equally applicable to the Caribbean and Americas region of the Commonwealth. These considerations include:

- Victims lack information on remedies. Offenders may warn targeted persons not to seek help, and victims/survivors may not know whom to contact for help or be too distraught or fearful to do so.
- Law enforcement help is limited. Cyberviolence investigation may require technological investigative skills that are lacking; victims/survivors may be told that there is little that law enforcement can do, especially if international communications are involved; law enforcement may lack awareness of the phenomena and of a gendered understanding of cyberviolence; incidents may be considered to be isolated and there may be a failure to realise that one incident is part of a larger pattern in which a perpetrator may be targeting numerous persons, and in many jurisdictions; only certain police forces may be equipped or authorised to investigate; national laws may not address certain types of attack, or police and prosecutors may not be aware how to apply existing laws to the phenomena.[201]
- Protection of children versus protection of adults. Some laws may only be applicable to protect children and not young adults, such as laws addressing child pornography and sexual exploitation of children.
- Role of social media providers. The cooperation of social media providers is required to identify and locate perpetrators; some platforms foster crime as a business model; some platforms are cooperative and offer mechanisms for content removals, etc., but in some cases, these may be too slow and widespread harm may have already occurred.
- Free speech versus hate speech. Countries may have different views, and even constitutional limitations, about the degree to which speech should be limited, and where to strike the balance between freedom of expression and personal and public safety. Thus, service providers in one country may be permitted to host certain content, which may be considered illegal in another country although accessible from the host country.

Part II Responses to Address Cyberviolence

8 Programme Responses

8.1 Digital Citizenship: Freedom of Expression, Sexual Expression and Social Responsibility

The internet is both good and bad. On the one hand, the internet provides children and young women with information about matters of sexual health, positive information about sexual activity and sexual identity, and 'for developmentally appropriate sexual curiosity and self-definition', and empowers young women and girls to promote their own 'sexual pleasure and autonomy'.[202] Sexting – sharing intimate photos between consenting parties – is often considered by many users of social media as a normal means of sexual expression and exploration, especially among youth. Witnesses reminded the Canadian Parliamentary Committee that 'it is important that young women and girls have equal access, compared to young men and boys, to the opportunities for expression, debate and personal development in the online realm'.[203] Similar sentiments were expressed by the IACHR, which described the internet as 'an essential tool for vulnerable or historically discriminated communities to obtain information, expose their grievances, make their voices heard, actively participate in public debate, and contribute to building public policy to rectify their situation'.[204]

On the other hand, sexual and other expression can be exploited by others to cause humiliation and embarrassment and ruin reputations. How does society draw the appropriate balance to permit the positive aspects of the internet while protecting its members from the harms of the negative aspects?

There are clearly cultural norms at play. As indicated earlier, many youths believe that cyberviolence is an inevitable component of the internet and mobile phone use.[205] Patriarchal norms and gender-based stereotypes exist, many of which shame and penalise women and girls for their sexual expression, thereby causing them to blame themselves. For example, victims are blamed and told that they are responsible for consensually sharing the intimate image in the first place.[206]

The Canadian Parliamentary Committee studying cyberviolence 'was reminded that adults are responsible for the design of the online environment, and for the societal and cultural norms in the offline world, which are reflected in the online world'.[207] The Committee was advised that:

> [T]here must be greater education and awareness of the concept of 'digital citizenship' whereby users of social media and ICTs understand and exercise their rights to safe and inclusive online communities as citizens and consumers. Developing a generation of good digital citizens includes teaching children and youth about empathy and respect online; showing children and youth that they have the ability to make a difference online; and sharing the steps they can take to oppose and report cyberviolence or hateful content.[208]

The remainder of this report will examine how society can promote positive 'digital citizenship' for all users and providers of online services, including online bystanders. The report of the UN Special Representative of the Secretary-General outlines several preventative responses to address cyberbullying, including legislation, government programmes, empowerment of children and education.[209] Again, the present report will limit itself to sources and findings in the Caribbean and Americas region of the Commonwealth.

8.2 Law Enforcement and the Justice System

Challenges to law enforcement and the justice system were noted in Section 7..[210] The Canadian Parliamentary Committee examining cyberviolence against young women and girls heard evidence about various measures that could be undertaken to address law enforcement challenges.[211] These included greater education of law enforcement and justice officials on cyberviolence, including training on how to employ existing legal frameworks to investigate and prosecute it. Additionally, suggestions were made for legislative reform to give these officials better legal tools to investigate and prosecute.

8.3 Community Services to Address Cyberviolence

It is important to realise that while individual perpetrators should be held accountable by criminal and civil laws for their conduct, the root causes are social issues involving equality-based human rights issues. Meaningfully addressing the disproportionate impact on women and girls requires social transformation to address misogyny, racism, homophobia and other intersecting socio-economic factors that have historically disadvantaged the achievement of equality.[212]

Programmes and initiatives must be designed to educate the youth to seek help and provide effective social services. For example, the Canadian Centre for Child Protection is a charitable agency designated by the Government of Canada to receive reports of online child exploitation through an online tip line (Cybertip.ca),[213] and acts in furtherance of legislation enacted to require mandatory reporting of internet child pornography by internet service providers.[214] It may also receive tips from the general public. However, the centre also provides a website and resources (NeedHelpNow) which allow any young person to access their services and understand what they can do, which safe adults are available to help them and how they can take down offending communications. Often, youth do not want to notify the police, and the website provides information for expeditious self-help.[215]

Greater education and awareness among the general population, as well as by young women and girls, is also required regarding cyberviolence. 'The goal of such awareness and education would be to help individuals identify at-risk situations online, limit individual's exposure to cyberviolence, mitigate damage after situations of cyberviolence, and to take action to change online culture to make cyberviolence unacceptable.'[216] This education needs to be founded on research. Some of the research projects noted by the Canadian Parliamentary Committee include:

- Project Shift, a national multi-year project led by YWCA Canada and funded by Status of Women Canada to create a safer digital world for young women;
- The eGirls Project, which examines girls' and women's experiences with online social media; and
- The Young Canadians in a Wired World research project, conducted by MediaSmarts, which analyses Canadian students' experiences with technology.[217]

Digital literacy is also an important element of awareness and education campaigns, which should:

- begin at a young age, as soon as children are interested in technology;
- teach youth critical thinking and decision-making skills;
- teach concepts of digital civility and being a 'good cyber-citizen';
- make distinctions between acceptable behaviour, unacceptable behaviour, and criminal behaviour online; for example, the difference between sexting and forwarding a sext without consent;
- inform youth how to recognise false and biased information because youth get most of their information from social media but are unlikely to take steps to authenticate it;
- provide information targeted at parents and teachers, enabling them to have regular conversations with children about the online realm, cyberviolence and cyber-safety; and
- teach youth how the online world functions, including information on online privacy, how to code, and how algorithms operate.[218]

Culture is propagated, if not also created, by the media. Accordingly, the media must also contribute to changing the harmful norms and stereotypes that underlie cyberviolence. It must uproot rape culture and promote positive cultural change.

'Media literacy should be provided to all children; in particular, young women and girls must be taught how to critically examine the popular culture messages, which tend to push for the hypersexualization of their bodies.'[219] Public awareness campaigns by government need to 'explain the impact that sexist and sexual images of women and girls in the media and pornography can have on gender relations, gender equality and violence against women and girls'.[220]

All of these measures would contribute to creating a positive digital citizenship for all providers and users, including bystanders.

8.4 Parliamentary/Government Reports and Recommendations

As indicated in this report, a Canadian Parliamentary Committee undertook a study and prepared a report on 'Taking Action to End Violence against Young Women and Girls in Canada', which included a specific chapter on cyberviolence. The report made a number of recommendations and observations. Those specifically relevant to online cyberviolence against women and girls include the following:

- 'The Government of Canada supports digital literacy organizations whose work aims to educate young people and their families on the dangers of cyberviolence, the potential risks of sexting, and healthy forms of sexual expression and informed consent in the online realm' (Recommendation 24, at p. 78).
- 'The Committee observed the need for a standardized curriculum in public schools that addresses sex positivity, healthy relationships, healthy sexuality, positive masculinity, pleasure, communication, intimacy, respect, bodily autonomy and healthy body image, and queer, trans and non-conventional experiences; and the need for the curriculum to be implemented in an age-appropriate and culturally appropriate manner as early as junior kindergarten' (Observation 3, at p. 78).
- 'The Committee observed the need for the implementation of a standardized curriculum in public schools that teaches digital and media literacy and that this curriculum: 1) prioritises the development of students' critical thinking skills towards media so that they are equipped with adequate tools and resources to critically examine the media and images they consume; 2) that it teaches concepts of digital civility and being a good digital citizen; and 3) that it makes distinctions between acceptable online behaviour, unacceptable online behaviour, and criminal online behaviour. Furthermore, this curriculum needs to be implemented in an age-appropriate and culturally appropriate manner as early as junior kindergarten' (Observation 4, at p. 78).
- Funding for both Legal Aid and the Victims Fund be increased and made available to survivors of gender-based violence in both civil and criminal law contexts (Recommendation 27, at p. 92; Recommendation 39 at p. 94).
- Educational curricula be developed, by the appropriate organisations, on gender-based violence and sexual assault, and on digital and media literacy, for law enforcement authorities, prosecutors and the judiciary (Recommendations 28, 29 and 30, at p. 92; Observations 5 and 6, at p. 94).
- The criminal offence of harassment be amended to make explicit that a fear for one's safety includes 'psychological safety and integrity' (Recommendation 33, at p. 93).
- The Government of Canada conduct a thorough meta-analysis of existing research on violence against young women and girls, with particular focus on, inter alia, hypersexualisation and cyberviolence, and 'allocate additional funding to research and data collection that focuses on intersectional violence against young women and girls in Canada, particularly in the areas of hypersexualisation, violent and degrading sexually explicit material, sex trafficking, street harassment, cyberviolence, violence on post-secondary campuses, and men and boys' views of gender-based violence' (Recommendations 39 and 40, at p. 98).

The Canadian Government has produced a National Action Plan on Violence against Women and Gender-based Violence, and recently released a final report on how to implement it.[221] Although not focused on cyberviolence, the report and its recommendations are instructive on how to address violence against women and gender-based violence.

Regarding the Caribbean region, the IACHR also stresses the importance of adopting strategies, laws and policies that promote education and awareness of cyberviolence, and combat stereotypes and discriminatory attitudes. States should 'take immediate steps to teach girls, in particular, how to use these technologies safely, by understanding their rights in the event of any act of violence and discrimination and knowing the multiple risks that exist online'.[222] Likewise,

teachers, parents, police, prosecutors and judges should be provided with appropriate educational training to understand and address acts of cyberviolence and discrimination. In addition to a set of comprehensive recommendations made to Latin American and Caribbean states on addressing, in general, violence against women and girls, the IACHR specifically recommended the need for further analysis of emerging forms of violence and discrimination, including hate speech and online violence.[223]

Another Canadian Parliamentary Committee undertook a study of online hate.[224] While the study and its recommendations are informative in respect of online hate against women and girls, the report did not specifically address this targeted group, but rather focused on all forms and targets of online hate. Its recommendations also address the need for better data collection, tracking of online hate, prevention, modernising the definition of hate and providing a new civil remedy in the Canadian Human Rights Act.[225] One recommendation, however, focused on establishing requirements for online platforms and Internet service providers:

> That the Government of Canada establish requirements for online platforms and internet service providers with regards to how they monitor and address incidents of hate speech, and the need to remove all posts that would constitute online hatred in a timely manner.
>
> - These requirements should set common standards with regards to making reporting mechanisms on social media platforms more readily accessible and visible to users, by ensuring that these mechanisms are simple and transparent.
> - Online platforms must have a duty to report regularly to users on data regarding online hate incidents (how many incidents were reported, what actions were taken/what content was removed, and how quickly the action was taken). Failure to properly report on online hate, must lead to significant monetary penalties for the online platform.
> - Furthermore, online platforms must make it simple for users to flag problematic content and provide timely feedback to them relevant to such action.[226]

8.5 Creating Positive Bystanders

A significant part of this report examined the phenomena of 'negative bystanders', that is, persons who redistributed harmful communications intentionally, recklessly or unwittingly. In Section 8.1, the notion of 'positive bystanders' was introduced; that is, persons who intervene to help. Sections 8.2–8.4 then examined the role of law enforcement and the justice system, community services and government recommendations, in particular the need for improved digital literacy and awareness of the problem, media intervention and education about acceptable and unacceptable online behaviour, all with the goal of creating active or 'positive bystanders'.

This section examines some of the strategies that have been developed to counter cyberviolence and encourage bystanders to take positive action.

Research has been undertaken in a number of countries about the 'bystander effect' (i.e., the disinclination to intervene to help).[227] Within the Caribbean and Americas region of the Commonwealth, one survey found that more than one in three Canadians say they have witnessed an act of cyberbullying (against a person they knew or someone they did not), but only a third intervened to help.[228] A Canadian university study found that:

> [I]n children of all ages there was a kind of moral disengagement when it came to the bystanders' role. They justified the bystanders' neutral behaviour by reasoning that moral rules don't apply in this particular context. Yes, the bystander should have stood up for his friend, but the bystander's friend would probably not stand up for him, so the bystander's neutral response is okay. (Some also justified the bully's behaviour by saying it was the morally correct thing to do. The bully behaved badly but it was for a good reason.)[229]

The study also found that the disinclination to intervene in, or report, a cyberbullying episode increased with the youth's age.[230]

Similar results have been found in Jamaica about the lack of seriousness given to cyberbullying, particularly by stakeholders in the education and public health sectors.[231]

One Canadian study (examining physical bystanders, rather than online bystanders) indicated that the greater the number of bystanders, the

less likely it is for any one of them to intervene. The greater diffusion of responsibility among onlookers resulted in less personal responsibility. Accordingly, it is important to take responsibility and 'to behave as if one is the first or only person witnessing a problem'.[232] Similar findings were found in an American research study on bystander intervention in cyberbullying. It found that 'accepting personal responsibility for witnessing cyberbullying was associated with greater odds that a person would flag cyberbullying', and that 'understanding the extent to which cyber-bystanders perceive that others will hold them accountable for their behaviour on a site meaningfully predicts acceptance of personal responsibility during cyberbullying'.[233]

A number of strategies have been developed within the Commonwealth Caribbean and Americas region to address the bystander effect. While most of these address workplace[234] or university harassment,[235] some address directly cyberviolence. For example, a Canadian university study developed a five-stage model to empower cyber-bystanders to become actively involved, which includes self-analysis of one's beliefs and reactions, and then designing cyberbullying strategies.[236] Likewise, an internet news article in Barbados provides six tips to deal with cyberbullying and online harassment, including from the perspective of the victim and a bystander.[237] Another Caribbean online post, originating in St Vincent and Grenadines, provides a number of tips on how to protect oneself against cyberstalking.[238]

UNESCO has launched a major international campaign to raise awareness and provide resources to counter the bullying of children, including cyberbullying.[239] It indicates that various programmes and campaigns have been carried out, including in North America, Latin America and the Caribbean.[240] Other strategies, in both Canada and the Caribbean, are also directed to assist teachers and parents in aiding children, as well as educating students.[241]

The national police force in Canada has a number of programmes to assist persons who experience or witness cyberbullying.[242] The Caribbean Institute for Security and Public Safety offers a wide range of training programmes for teachers, social workers, guidance counsellors, law enforcement and other public safety officers in many subject areas, including cyberbullying.[243] A training manual to counter cyberstalking, revenge porn and other cyber abuses has been launched in Barbados.[244]

Recently, the Canadian Government launched a new campaign against online child sexual exploitation to raise awareness of the issue with children and their guardians, and to increase reporting to the national tip line on child sexual exploitation. The strategy includes videos and resources for educators, youth and parents/guardians.[245]

9 Proposed Law Reforms

9.1 Proposed Criminal Law and Regulatory Reforms

9.1.1 Cyberbullying and the Non-consensual Distribution of Intimate Images

As noted earlier, Canada's Criminal Code contains a number of offences (technologically neutral) that are equally applicable to the phenomena of cyber-harassment/cyberbullying, and a specific criminal offence, and related procedural remedies, for the non-consensual distribution of intimate images, all of which apply nationally. Additionally, a number of provinces have enacted both penal and civil relief statutes under their legislative powers to address the distribution of intimate images, of which some provisions also address cyberbullying.[246] All of these measures were preceded by a law reform report of a federal-provincial-territorial working group of justice officials, which provides significant insight into the legal principles, philosophical underpinnings and rationale of these criminal/penal statutes.[247]

Commonwealth jurisdictions interested in considering law reform in the area of criminal or penal offences addressing cyberbullying/harassment, and the distribution of intimate images, are recommended to examine these statutes and to refer to the report of the federal-provincial-territorial working group.

Trinidad and Tobago proposed the enactment of a new cyberbullying offence to criminalise a person who 'uses a computer system to communicate with the intention to cause harm to another person'. Harm is proposed to mean 'serious emotional distress'. In determining whether an offence has been committed, a judge can consider various factors, including extremity of language, age and characteristics of persons involved, anonymity of the communication, repetition of communication, extent of circulation, truth/falsity of the communication and context in which the communication appeared.[248] Some concern

has been expressed that this proposal could chill freedom of expression where exposure of wrongdoing of public officials causes them 'serious emotional distress'.[249]

Trinidad and Tobago also proposed the enactment of a new offence to criminalise voyeurism and the non-consensual distribution of intimate images. It would penalise a person who intentionally, without lawful excuse and without consent, captures, stores, publishes or transmits through a computer system, the image of 'the private area' (defined as 'the genitals, pubic area, buttocks or breast') of another person, where there is reasonable expectation of privacy to disrobe or that the private area would not be visible, whether in a public or private place.[250]

HIPCAR has proposed a model provision to criminalise a person who, without lawful excuse or justification (or excess thereof), initiates an electronic communication by using a computer system to support severe, repeated and hostile behaviour, 'with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person'.[251] This proposal would address some forms of cyberviolence involving cyberbullying, harassment and intimidation.

It should be noted that these three proposals, as well as most of the laws in the Caribbean region (discussed above), are limited to commission through a computer system, and may not – depending on the jurisprudence and rules of interpretation of relevant statutory provisions used in the different countries – capture the same conduct committed by means of other telecommunication systems, such as telephones,[252] or other oral or written communications in the physical world.

As noted earlier, British Virgin Islands amended its computer crime law to extend its application to telephone mobile networks. This is something that should be examined further by all Caribbean jurisdictions.

In Canada, existent general offences of harassment, intimidation, uttering threats, extortion, fraud, forgery, identity theft, voyeurism and non-consensual distribution of intimate images are technologically neutral and apply equally in the offline and online realms.[253]

As distinctions are often artificial or meaningless as between the physical world and cyber realm, reforms should be technologically neutral (i.e., not restricted to computer systems and the 'cyber' electronic realm), to the greatest extent possible, as similar violence often occurs in both offline and online spheres or originates in one sphere and is carried through into the other.

9.1.2 Other Forms of Cyberviolence

Both Trinidad and Tobago and HIPCAR have proposed computer-related offences that would address other forms of cyberviolence (discussed in Part II).

Both Trinidad and Tobago, and HIPCAR, proposed the enactment of an identity-related offence to criminalise the intentional transfer, possession or use of another person's identification, and also a computer-related forgery offence, which could address cyberviolence involving the creation of fake websites or impersonation of a targeted person.[254]

Trinidad and Tobago also proposed a new offence of illegal acquisition of computer data, which could address some forms of cyberviolence involving access or interception of a person's data or computer communications.[255] This proposal, however, has been criticised for its vague terminology and possible impact on journalists and whistle-blowers with respect to leaks of government information and corporate corruption.[256] HIPCAR has also proposed an offence of illegal access to a computer system, as well as interception of computer transmissions.[257]

Trinidad and Tobago also proposed an offence to criminalise threats to publish 'computer data containing personal or private data which can cause public ridicule, contempt, hatred or embarrassment', with intent to extort a benefit from a person.[258] This would address some forms of sextortion.

HIPCAR proposed computer-related child pornography offences, which would address some forms of cyberviolence involving sexual exploitation.[259]

Again, as discussed in Section 9.1.1, all of the proposals noted earlier are computer related, and may not address cyberviolence utilising other telecommunication systems, such as mobile telephones, or oral and written communications in the physical world. To the greatest extent possible, reforms should be technologically neutral to capture similar conduct in both the offline and online realms. This should be examined further.

Lastly, both Trinidad and Tobago, and HIPCAR, propose other computer-related offences that would give effect to the Commonwealth Model Law on Computer and Computer Related Crime, which could be used to address some of the other forms of cyberviolence discussed in Part II.

Jurisdictions should also consider the analysis and recommendations of a 2019 report on cybercrime strategies and policies for the Caribbean community.[260]

On 23 June 2021, the Canadian Government introduced a Bill in the House of Commons to improve legal remedies for victims of hate speech and hate crimes. The Bill proposes to amend the Canadian Human Rights Act to enable the Canadian Human Rights Commission and Canadian Human Rights Tribunal to review and adjudicate hate speech complaints. The Bill also proposes amendments to the Criminal Code to provide a definition of 'hatred' for the existing hate propaganda offences, and to create a new judicially ordered peace bond (i.e., restraining order) to prevent the commission of hate propaganda and hate-motivated crimes.[261]

9.1.3 Regulation of Social Media and ICT Platforms

On 29 July 2021, the Government of Canada issued a press release[262] launching a public consultation on proposed legislative options to promote a safe and inclusive online environment, while protecting the freedom of expression and privacy. The government also declared that it intended to table a bill later in the year (2021) to establish a legislative and regulatory framework to make social media platforms and online services more accountable and transparent in addressing harmful online content.

The announcement also included the release of a Discussion Guide that outlines the proposals, including various options under consideration by the government, and seeks public comment.[263] The proposed legislation would apply to 'online communication service providers', which would be included/excluded by regulation; the intent being to capture major platforms, but exclude some websites that simply provide products or services (e.g., travel reviews) and telecommunication service providers. The legislation would target five types of harmful content: terrorist content, content that incites violence, hate speech, non-consensual sharing of intimate images and child sexual exploitation content. Regulated entities would be required to take all reasonable measures to make harmful content inaccessible, by monitoring for regulated categories of harmful content, flagging content, assessing whether it meets the criteria for rendering it inaccessible and, if met, rendering it inaccessible. Regulated entities would be required to establish notice and appeal systems for both authors of content and those who flag it for the attention of the online communication service provider. Regulated entities would also be required to be more transparent, by publishing data on volume and type of data dealt with at each step of the process, and on the development, implementation and updating of their guidelines.[264]

The proposed legislative amendments would also create specific obligations to assist law enforcement and national security agencies to permit appropriate investigative and preventative action. Various options are proposed for consideration to require regulated entities either to notify or report to these agencies regarding the presence of potentially illegal content on their platforms which falls within the five categories of harmful content (options involve various levels of threshold and suspicion/belief to trigger the obligation).[265] Regulated entities would be required to preserve regulatory-prescribed information that could support an investigation including transmission data (i.e., IP address, date, time, type, origin and destination of the material), basic subscriber information (i.e., customer name, address, contact and billing information) and the content itself. Various options are also considered for mandatory reporting of such information to law enforcement agencies (without the need to obtain judicial orders), where the content involves child pornography.[266]

The proposed legislation would create a new set of regulators. A new Digital Safety Commission of Canada, led by a digital safety commissioner, is proposed to operationalise, oversee and enforce the new regime, including leading research and programming, collaborating with stakeholders and supporting regulated entities. A Digital Recourse Council would provide independent recourse and an appeal avenue for the content moderation decisions of regulated entities, with binding decisions. An Advisory Board would also be established to provide both the commissioner and the Recourse Council with expert advice to

inform their processes and decision-making. The composition of the board would be diverse subject matter experts from civil society, legal experts, equity-seeking communities, Indigenous peoples, civil liberties, advocacy groups, industry and academia.[267]

10 Proposed Civil Law Reforms

10.1 Non-consensual Distribution of Intimate Images

In 2020, The Uniform Law Conference of Canada[268] adopted a Report and a Draft Uniform Non-consensual Disclosure of Intimate Images Act,[269] for the consideration of provincial and territorial legislatures, which proposes the creation of a new statutory tort to address the non-consensual distribution of intimate images, as well as the threat to distribute such. The new tort would be actionable without proof of damage,[270] and provides two statutory means of initiating legal proceedings.

The first proposal is for an inexpensive fast-track proceeding initiated by way of application to a court seeking (1) a declaration that the distribution of relevant images is unlawful; and (2) injunctive relief for the removal of the images from relevant ICT platforms, either by the person who distributed them (respondent) and/or the internet intermediary platform that hosts or indexes the content. A court may also order the respondent to pay nominal damages.

This tort proceeding would be one of strict liability, as the applicant need only prove that the respondent distributed the image of the applicant. There would be no requirement to prove non-consensual distribution or damage, and lack of intent to publish and lack of knowledge would not be a defence.[271] The primary goal of this tort application is to permit victims to obtain an inexpensive means to destroy, remove or deindex the images.

The second proposal is for a traditional fault-based tort cause of action, initiated by a cause/claim of action. In addition to providing the same type of declaratory and injunctive relief that the fast-track tort application provides, this claim of action would also provide for a court to order the respondent to pay comprehensive damages, including compensatory, aggravated and punitive damages. A person can proceed by both tort mechanisms, first obtaining expeditious removal and then seeking comprehensive damages after a full trial.[272]

With respect to both tort proceedings, while the applicant/plaintiff must prove that she is depicted, it is not necessary that the applicant/plaintiff be identifiable by a third party (such as directly by face-image or other body characteristics, or indirectly by identifiable surroundings linked to her identity, e.g., a particular bedroom environment), if she can prove to the court that her body is depicted in the image. The rationale for this proposal is that she knows it is an image of her, and while not clearly identifiable of her today, she suffers the harm of living in fear that she may be identified at a future time. The applicant/plaintiff should be able to seek relief 'without having to wait until they are identifiable and the worst damage possible is inflicted', as the two tort proceedings address both reputational harm and privacy invasion.[273]

Unlike the current statutes, the definition of 'intimate image' is expanded to include 'nearly nude' images, if there was a reasonable expectation of privacy at the time that the image was recorded and, if distributed, at the time of distribution. This could capture dressing/undressing and 'upskirting' images, but not include a woman or girl wearing a bikini on a public beach.[274] The definition of 'intimate images' would also include altered images, such as those created by deep or shallow/cheap fakes.[275] According to the report, the definition should not include wholly original content, such as nude drawings or paintings of individuals;[276] however, this interpretation is not expressly clear in the definition.

As the proposed legal remedies are civil in nature, rather than criminal/penal, the respondent would have the burden of proof that the applicant/plaintiff did not have a reasonable expectation of privacy in the recording or distribution of the image.[277] A presumptive publication ban to protect the identity of the applicant/plaintiff must also be ordered by the court, unless the applicant/plaintiff requests that there not be a publication ban.[278]

With respect to defences, a person is not liable for the application-based tort if the person can prove that the individual depicted in the intimate image consented to the distribution.[279] A person is not liable for the claim of action-based tort if the person proves that they (1) did not intend to distribute; (2) honestly and reasonably believed that the individual depicted had consented to the distribution; or (3) the distribution was made in the public interest and did not extend beyond the public interest.[280] The differences in the defences are attributable to the fact that the first tort

proceeding's goal is the expeditious destruction or removal of the intimate image, while the other is to hold the respondent civilly responsible for harm and damages. The defence of consent in both tort proceedings focuses on whether the complainant consented to the distribution, as assessed objectively. This is in contrast to some existing criminal/penal statutes that instead focus on the accused's/respondent's subjective knowledge or recklessness as to whether consent existed, as these laws relate to criminal/penal culpability and fault of the distributor's conduct.[281] For both tort proceedings, consent is revocable and, if revoked, the person who distributed must make reasonable efforts to make the image unavailable to others, and may be liable for any injury resulting from such failure. This is important in those situations where, although creation and distribution may have originally been consensual, an intimate relationship ends or becomes abusive, and consent is withdrawn for further use or distribution of the images.[282]

'No application or claim of action may be brought against an internet intermediary ('an organisation that hosts or indexes third party content through an online platform'), if the internet intermediary has taken reasonable steps to address unlawful distribution of intimate images in the use of its services.' However, the internet intermediary may still be subject to the declaratory and injunctive relief sought in an application or claim against another person, and be ordered to destroy, remove or deindex the image.[283] LEAF argues that this limitation of liability only applies to organisations, the business model of which involves the ordinary function of facilitating transactions among third parties and which have taken reasonable steps to address unlawful distribution in the use of its services; thus, the limitation of liability would not apply to individuals who specifically set up a website that primarily hosts or indexes non-consensually distributed intimate images. In such cases, tort applications and claims of action with these individuals named as respondents should be possible.[284]

While the draft model law is silent with respect to online bystanders, nothing in the text of the model law would appear to prevent an online bystander being targeted as a respondent in any of the two tort proceedings, if the bystander distributed, or threatened to distribute, an intimate image.

10.2 Defamation in the Internet Age

In 2020, the Law Commission of Ontario (LCO) published a final report, after a four-year project, examining the legal and policy issues intersecting defamation tort law in the province of Ontario and the impact of the Internet and social media.[285] The report makes 39 recommendations designed to update defamation law, promote access to justice and promote intermediary responsibility for defamatory internet speech. The recommendations are guided by seven principles:[286]

1. Defamation law must rebalance protection of reputation and freedom of expression in the internet age: a new balancing of protection of reputation and freedom is necessary.
2. Defamation law needs to be updated: a comprehensive new statutory legal framework should be enacted to respond coherently to new forms of communication.
3. Defamation law is evolving, and reforms must be complementary: with a few exceptions reworking the substantive law is not necessary; the primary problem in the law is procedural barriers.
4. Access to justice and dispute resolution must be improved: alternate dispute mechanisms are needed to divert high-volume and low-value defamation claims away from the formal court system.
5. Defamation law must specifically address online personal attacks: traditional defamation law and principles and court processes, developed over time to respond to media law cases, are inadequate when applied to online personal attacks.
6. New obligations should be created for intermediary platforms: two distinct duties are proposed for intermediary platforms – the obligation to pass on a notice of a defamation complaint to the publisher of the content, and the obligation to itself remove the content subject to a notice if the publisher does not respond to the notice.
7. Defamation and privacy law have distinct objectives and should remain separate.

To resolve defamation disputes in the internet age, three procedural streams are proposed. The first stream, notice and takedown, would permit a

complainant to notify an intermediary platform of alleged defamatory content hosted on its platform, and the intermediary platform would, among other duties, be required to pass the complaint to the publisher. If the publisher does not respond, the platform would be obligated to take down the offending content. The second stream would provide rules to encourage informal negotiations between the complainant and publisher, which could possibly be aided eventually by a new, voluntary, online dispute resolution tribunal. The third stream, a traditional court action, would be available primarily (but not exclusively) for higher-value claims.[287] In addition to existing interlocutory motions, a new interlocutory takedown order is recommended where 'the potential for reputational harm is so serious that the public interest in taking down the expression outweighs the public interest in the defendant's freedom of expression'.[288]

The report also makes recommendations regarding the law of jurisdiction in multistate defamation actions and choice of law. It also reviews platform liability regimes in other jurisdictions (e.g., the USA, European Union and United Kingdom), and rejects these regimes for adoption in Canadian law.[289]

The LCO report also proposed some substantive changes to the elements of defamation tort law, such as abolishing the distinction between libel and slander. While the common law test for defamation, and the common law presumptions of damage and falsity, should remain, the report recommends that courts should explicitly consider the overall context of the online content and degree of sophistication of the readers. The defence of fair comment should be simplified and renamed the defence of opinion.

The LCO report also proposed reforms regarding the common law doctrine of publication, which would have implications in situations where bystanders may be involved to various degrees with original publishers. Under the common law, publishers are generally understood to include not only individuals who are directly responsible for the communication, but also 'individuals who repeat, republish, endorse, or authorise it, or in some other way participate in its communication. The doctrine is increasingly incoherent in the online context, where there is a web of actors who may be peripherally involved in the communication of defamatory content but may not be considered sufficiently blameworthy to ground liability.'[290] Therefore, the LCO report recommends replacing the common law definition with a statutory definition of publisher, such that 'only actors having the intent to convey a specific expression at the time of publication should be considered publishers and, therefore, subject to liability in defamation law'.[291] Therefore, a publisher of defamatory material should be liable for a republication by a third party (e.g., an online bystander) only where the original publisher intended the material to be republished. Likewise, where an online bystander republishes in circumstances that meet the definition of defamation, they too could be subject to any changes to defamation law in accordance with the proposed reforms in the LCO report.

While LEAF welcomed the LCO report as a significant contribution to inform Canadian law regarding platform liability, they expressed some caveats about the report's analysis and application to gender-based violence against women and girls.[292] First, any application of defamation law should not conflate cyberviolence-related defamation with 'other kinds of defamation that do not involve systemic oppression or historical inequity'. Second, any application of defamation law should remain 'sensitive to how it has been exploited to silence victims/survivors of sexual assault and intimate partner violence and prevent future victims/survivors from speaking out'. Third, an intersectional feminist analysis of defamation law would need to examine how 'reputation is publicly perceived, harmed, bolstered, or protected, depending on one's gender, race, disability, sexual orientation, and class'. Fourth, defamatory expression that 'attempts to weaponise the targeted person's sexuality against them' should be examined for underlying misogynistic and other biased assumptions against gender equality, and to what extent defamation law upholds those assumptions.[293]

Part III Conclusions

This report has revealed that cyberviolence against women and girls in the Caribbean and Americas region of the Commonwealth is recognised as a serious problem, and that measures are being taken to address it.

This report has canvassed various types and modes of cyberviolence and analysed their impact on women and girls. Cyberviolence is prevalent and is gender based in terms of its root causes and impact. It certainly has a disproportionate impact on women and girls and marginalised individuals, in particular where there is also intersectionality of race, ethnicity, religion, sexual orientation, poverty, disability and other socio-economic factors that unfairly increase their marginalisation. It results in various types of physical, emotional, psychological and medical health, sexual and socio-economic harms for the targeted person and their families. It can also negatively affect the person's public and democratic participation in society, both online and offline. Similar types of violence against women and girls often occur in both offline and online spheres or originate in one sphere and are carried through into the other. In the most serious cases, cyberviolence can lead to the commission of physical assaults, and even cause some people to commit suicide.

To various degrees, current legal frameworks in Commonwealth countries in the Caribbean and Americas region criminalise some forms of cyberviolence or provide civil remedies. However, significant gaps exist in many jurisdictions, as compared with those jurisdictions that have a more robust legal framework that can be applied to address cyberviolence. Some jurisdictions have enacted specific new offences and statutory civil remedies to address some forms of cyberviolence, such as harassment/cyberbullying/stalking and the non-consensual recording or distribution of intimate images, and a few other jurisdictions have proposed to enact more comprehensive legal remedies. Some of the crimes in the Commonwealth Model Law on Computer and Computer Related Crime may also address some forms of cyberviolence, and a number of jurisdictions have enacted legislation that aligns with the model law. Traditional common law torts, such as the law of defamation, may also apply to provide some civil remedy. Some recent developments have occurred in one jurisdiction, Canada, 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.

The majority of jurisdictions could benefit by examining the enactments or proposals of the few jurisdictions that have acted comprehensively.

With respect to online bystanders, some may be recruited, 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. It is, therefore, important that any legal, educational and preventative measures recognise the various distinctions in the level of moral responsibility and culpability of bystanders.

With respect to the criminal liability of bystanders, some jurisdictions have clearly articulated statutory rules in penal codes, or cybercrime laws, regarding participation in the commission of an 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 awareness (i.e., intent, knowledge, 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, a facilitator or an inciter or procurer.

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 are systemic social and cultural norms involving equality-based human rights issues. Meaningfully addressing the disproportionate impact on women and girls requires social transformation to address the negative culture of misogyny, sexual exploitation, gender-based stereotypes and discrimination, homophobia, racism, discrimination against minority groups and other intersecting socio-economic factors that have historically disadvantaged the achievement of equality.

Responses to address cyberviolence vary across the Caribbean and Americas region, with some jurisdictions being more active than others. Some jurisdictions have implemented some programmes developed by law enforcement, government, community organisations or the ICT industry, and at least one jurisdiction has conducted extensive parliamentary studies and reports with recommendations for action to address cyberviolence against women and girls. These programmes have the goal of creating positive digital citizenship and responsibility, whereby users of social media and ICTs understand and exercise their rights to safe, responsible and inclusive online communities as citizens and consumers. 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. 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. 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.

Within the purview of law ministers' mandates, some law reforms have been enacted by jurisdictions in the Caribbean and Americas region (as noted above), and other reforms have been proposed, to address and penalise various forms of cyberviolence, such as cyber-harassment, cyberbullying, intimidation, recording and distribution of intimate images, identification theft and fraud, access to personal data, sextortion, sexual exploitation and hate speech, as well as related procedural and judicial powers to provide remedies. Some of these laws have been criticised for negatively affecting freedom of expression, due to the breadth or ambiguity of the statutory language employed. In one jurisdiction, Canada, law reforms have been proposed regarding the role and regulation of social media and ICT platforms. In the same jurisdiction, reforms have been proposed to create a new statutory tort and civil remedies to address the non-consensual distribution of intimate images, and to have tort laws on defamation and court processes fit for the Internet age.

Accordingly, Commonwealth countries in the Caribbean and the Americas regions may in collaboration with the Commonwealth Secretariat :

1. Develop comprehensive model laws/model legal provisions (both criminal and civil) to assist Commonwealth jurisdictions to address various forms of 'cyberviolence', while balancing other rights, such as freedom of expression. As distinctions are often artificial or meaningless as between the physical world and the cyber realm, these reforms should be technologically neutral (i.e., not restricted to computer systems and the 'cyber' electronic realm), to the greatest extent possible, as similar violence often occurs in both offline and online spheres, or originates in one sphere and is carried through into the other.

2. Undertake a study of social-psychological research on cyberviolence, such as cyber-harassment/cyberbullying and the non-consensual distribution of intimate images. 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 also examine how to prevent cyberviolence by online bystanders, and how to promote positive digital citizenship and responsibility, through education and other preventative measures. The study should also examine the various modes of participation in the commission of an offence, given that some online bystanders are negative bystanders. 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 and the United States.

3. Considering the results of the social-psychological research (recommended above), adopt a multi stakeholder approach, working with other government ministries, including those responsible for law enforcement, education and social services, to develop (for both government and community organisations) social and educational programmes to address cyberviolence and to promote digital citizenship 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' analytical lens (i.e., an analysis taking into account gender-based and other intersecting identities).

References

1 'Interpersonal Cybercrime Prevention', UNODC, https://www.unod.org/e4j/en/cybercrime/module-12/key-issues/interpersonal-cybercrime-prevention.html.

2 Council of Europe Convention on Violence against Women and Domestic Violence (CETS 210), (Istanbul Convention), http://www.coe.int/en/web/conventions/full/-list/-/conventions/treaty/210.

3 Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against women, (the Belém do Para Convention), https://www.oas.org/juridico/english/treaties/a-61.html.

4 'Violence against Women', UN 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, [FR] Etude cartographique sur la cyberviolence (July 2018) p. 5, www.coe.int/cybercrime (hereinafter 'Council of Europe').

6 'Violence and Discrimination against Women and Girls: Best Practices and Challenges in Latin America and the Caribbean', Inter-American Commission on Human Rights, Organization of American States (2019), p. 134 http://www.oas.org/en/iachr/reports/pdfs/ViolenceWomenGirls.pdf , (hereinafter 'IACHR').

7 '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. 32, file://localhost/C:/Users/Admin/Documents/Commonwealth/hoc%20report%20on%20violence%20aginst%20women%202017.pdf (hereinafter 'Canadian Parliamentary Committee').

8 IACHR, p. 134.

9 Canadian Parliamentary Committee, p. 32. See also IACHR, p. 134.

10 Cynthia Khoo, 'Deplatforming Misogny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence, Women's Legal Education and Action Fund (LEAF) (April 2021), p. 15, https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf (hereinafter 'LEAF'); see also: Jessica West, 'Cyber-Violence against Women' (May 2014) pp. 2 and 16, Battered Women's Support Services, http://www.bwss.org/wp-content/uploadeds/2014/05/CyberVAWReportJessicaWest.pdf.

11 Ibid.

12 Canadian Parliamentary Committee, p. 32.

13 See also IACHR, p. 134.

14 E.g., Antigua and Barbuda, Electronic Crimes Act 2013 and Computer Misuse Act 2006; Barbados, Computer Misuse Act 2005 and Telecommunications Act 2001 Cap 282B; Canada, Criminal Code of Canada RSC 1985 cC46 and the Telecommunications Act (S.C 2010, c23); Grenada, Electronic Crimes Act 2013; Jamaica, Criminal Justice Act 2014 and the Cybercrime Act 2010; Guyana, Cybercrime Act 2018 and Sexual Offences Act 2010; Saint Lucia, Criminal Code 2004; British Virgin Islands, Computer Misuse and Cybercrime (Amendment) Act 2019; St Vincent and the Grenadines, Electronic Evidence Act 2004 and Cybercrime Act 2016; St Kitts and Nevis, Electronic Crimes Act 2009; Trinidad and Tobago, Computer Misuse Act 2000 and Cybercrime Bill 2017.

15 Council of Europe, p. 6 (see graphic diagram).

16 Council of Europe, p. 4.

17 Council of Europe, p. 6.

18 LEAF, p. 16.

19 LEAF, p. 16.

20 Council of Europe, p. 7.

21 LEAF, p. 16.

22 Dubravka Šimonović, '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.

23 Canadian Parliamentary Committee, p. 33. See also LEAF, p. 29.

24 Council of Europe, pp. 7–8 (italic emphasis added). See also: 'Annual Report of the Special Representative of the Secretary-General on Violence against Children', UN Human Rights Council, 31st session (2016), for a description of cyberbullying and its impact on children, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Documents/A_HRC_31_20_E.doc.

25 LEAF, p. 19 (italic emphasis added).

26 'Cyberbullying and Youth', *Trinidad and Tobago Guardian* (2015), p. 1, https://www.guardian.co.tt/article-6.2.376401.37bb05bd92.

27 Council of Europe, p. 7.

28 Canadian Parliamentary Committee, p. 33.

29 LEAF, p. 20 (and see footnote p. 40 cited therein).

30 LEAF, p. 21.

31 'Cyber Law in the Caribbean (Part 2)', p. 3 and 4, https://thenmlssalitigator.wordpress.com/2015/02/26/cyber-law-in-the-caribbean-part-2/.

32 LEAF p. 17.

33 LEAF, p. 17 at footnote 18. See also: Dubravka Šimonović, '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. 41.

34 Council of Europe, p. 10; Canadian Parliamentary Committee, p. 34.

35 Council of Europe, p. 11. See also 'Cyber Bullying Laws', https://www.hg.org/legal-articles/cyber-bullying-laws-40713.

36 LEAF, p. 18. See also 'The Facts about Online Hate and Cyberviolence', Canadian Women's Foundation, https://canadianwomen.org/the-facts/online-hate-and-cyberviolence.

37 Ibid.

38 *R. v. Jarvis*, [2019] S.C.R. 10, at paras. 60–61; RSC 1985, c. C-46, s. 162(1).

39 LEAF, p. 17.

40 Canadian Parliamentary Committee, p. 34.

41 LEAF, p. 18.

42 LEAF, p. 19.

43 Ibid.

44 Ibid.

45 LEAF, p. 17; see also Canadian Parliamentary Committee, p. 34.

46 Council of Europe, p. 11. See also: Hodine Williams and Andrae Campbell, 'A Punch at Cyber Bullying', *Jamaica Observer* (2016), p. 2, https://www.jamaicaobserver.com/news/a-punch-at-cyber-bullying_78983.

47 Council of Europe, p. 12.

48 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.

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

50 See also: Canadian Parliamentary Committee, p. 34; LEAF, p. 21; and Dubravka Šimonović, '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. 32.

51 IACHR, p. 135.

52 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.

53 'Cybercrime/E-crimes: Model Policy Guidelines and 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.

54 LEAF, p. 16.

55 'Taking Action to End Online Hate', Report of the Standing Committee on Justice and Human Rights, 42nd Parliament, 1st Session, June 2019 (Anthony Housefather, Chair).

56 Council of Europe, p. 13; LEAF, p. 16.

57 Council of Europe, p. 13.

58 Council of Europe, p. 14; See also LEAF, p. 20.

59 LEAF, p. 20.

60 Council of Europe, p. 19.

61 LEAF, p. 19.

62 Canadian Parliamentary Committee, p. 34.

63 LEAF, p. 20.

64 LEAF, p. 23.

65 Ibid.

66 Plan-international (2020) 'Abuse and Harassment Driving Girls off Facebook, Instagram and Twitter', https://plan-international.org/news/2020/10/05/abuse-and-harassment-driving-girls-off-facebook-instagram-and-twitter/.

67 Ibid.

68 E.g., 'Caribbean Women Count: Ending Violence against Women and Girls Data Hub', UN Women, https://caribbeanwomencount.unwomen.org; 'A Report to Guide the Implementation of a National Action Plan on Violence Against Women and Gender-Based Violence', Women's Shelters Canada (April 2021), https://www.nationalactionplan.ca/wp-content/uploads/2021/06/NAP-Final-Report.pdf.

69 'The Facts about Online Hate and Cyberviolence', Canada Women's Foundation (2019), https://canadianwomen.org/the-facts/online-hate-and-cyberviolence/.

70 Canadian Parliamentary Committee, p. 35 (footnote references omitted).

71 'Government of Canada Awareness Campaign Addresses Growing Risk of Online Child Sexual Exploitation', Public Safety Canada (12 July 2021), https://www.canada.ca/en/public-safety-canada/news/2021/07/government-of-canada-awareness-campaign-addresses-growing-risk-of-online-child-sexual-exploitation.html.

72 Statistics Canada, 'Cyberbullying and Cyberstalking among Internet Users Aged 15 to 29 in Canada,' in Darcy Hango, *Insights on Canadian Society* (19 December 2016), p. 3. See also Canadian Parliamentary Committee, p. 35.

73 Ibid., p. 4.

74 'Cyberstalking in Canada', Statistics Canada, https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2017039-eng.htm.

75 Ross Sheil, 'Jamaican Children and the Hidden Dangers of Online Abuse' (2016), p. 2, https://blogs.unicef.org/jamaica/unspoken-jamaican-children-online-abuse/.

76 Inid., p. 2; and see also 'Caribbean Girls under Cyber Attack', Silcon Caribe (2017), https://www.siliconcaribe.com/2017/05/04/caribbean-girls-under-cyber-attack/.

77 Hodine Williams and Andrae Campbell, 'A Punch at Cyber Bullying', *Jamaica Observer* (2016), p. 2, https://www.jamaicaobserver.com/news/a-punch-at-cyber-bullying_78983. However, the source and which countries were surveyed is not disclosed.

78 'Alarming Figures of Bullying in Latin America and the Caribbean', *LatinAmerican Post* (2018), p. 4, https://latinamericanpost.com/24051-the-alarming-figures-of-bullying-in-latin-america-and-the-caribbean.

79 LEAF, p. 21 (footnote references omitted). See also: Dubravka Šimonović, '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) at 25; Jane Bailey, Valerie Steeves and Suzanne Dunn, 'Submission to the Special Rapporteur on Violence against Women re: Regulating Online Violence and

Harassment Against Women' (September 2017) at paras 7 and 13e, eQuality Project, http://www.equalityproject.ca/wp-content/uploads/2017/12/Bailey-Steeves-Dunn-Submission-27-Sp-2017.pdf; Adam Cotter and Laura Savage, 'Gender-based Violence and Unwanted Sexual Behaviour in Canada, 2018: Initial Findings from the Survey of Safety in Public and Private Spaces', Juristatm Catalogue No 85-002-X (Ottawa: Statistics Canada, 2019).

80 T. Smith and N. Stamatakis, 'Cyber-victimization Trends in Trinidad and Tobago: The Results of an Empirical Research', *International Journal of Cybersecurity Intelligence & Cybercrime*, 4(1) (2021), 46–63, at pp. 51–53 and pp. 58–59.

81 Ibid., p. 58.

82 Ibid., pp. 59–60.

83 Ibid.

84 The ECA consists of 12 islands of which 8 are independent states (Saint Kitts and Nevis, Dominica, Antigua and Barbuda, Grenada, Saint Vincent and the Grenadines, Saint Lucia, Barbados and Trinidad and Tobago), and 4 are UK Overseas Territories (Montserrat, Anguilla, British Virgin Islands, and Turks and Caicos Islands).

85 'Alarming Figures of Bullying in Latin America and the Caribbean', *LatinAmerican Post* (2018), p. 4, https://latinamericanpost.com/24051-the-alarming-figures-of-bullying-in-latin-america-and-the-caribbean.

86 'Violence against Children (VAC) in the Eastern Caribbean Area', UNICEF (2020), p. 11, http://www.iin.oea.org/pdf-iin/materiales-resentaciones/VAC%20in%20the%20Eastern%20Caribbean%20Area.pdf.

87 N. Metri, 'Building Awareness of Digital Violence against Barbadian Women', *Internet Society* (2018), https://www.internetsociety.org/blog/2018/07/building-awareness-of-digital-violence-against-barbadian-women/.

88 LEAF, p. 22. And see: Women's Shelters Canada, 'Shelter Voices' (June 2017), p. 3, https://endvaw.ca/wp-content/uploads/2017/06/shelterVoices_ENG_2017WEB.pdf.

89 LEAF, pp. 32–35. (Citations to the court cases as referenced in the footnotes have been omitted here but are available in the original LEAF report. Asterisks have been substituted to indicate the presence of citations to court cases.)

90 TFGBV is an abbreviation for 'technology-facilitated gender-based violence'.

91 Hodine Williams and Andrae Campbell, 'A Punch at Cyber Bullying', *Jamaica Observer* (2016), p. 2, https://www.jamaicaobserver.com/news/a-punch-at-cyber-bullying_78983.

92 'Annual Report of the Special Representative of the Secretary-General on Violence against Children', UN Human Rights Council, 31st session (2016), for a description of cyberbullying and its impact on children, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Documents/A_HRC_31_20_E.doc.

93 Jane Bailey, Valerie Steeves and Suzie Dunn, 'Submission to the Special Rapporteur on Violence against Women re: Regulating Online Violence and Harassment Against Women' (27 September 2017) as cited in LEAF, p. 24.

94 Canadian Parliamentary Committee, pp. 36–38; LEAF, p. 24; 'Impacts and Consequences of Bullying and Cyberbullying', Royal Canadian Mounted Police, p. 2, https://www.rcmp-grc.ca/en/bullying/impacts-and-consequences-bullying-andcyberbullying. Rehtaeh Parson was sexually assaulted by four classmates at a teen party. The boys took photos of the assault and distributed them to her classmates. They were subsequently convicted of producing and distributing child pornography (due to evidentiary issues, the prosecution did not proceed with sexual assault charges). Amanda Todd was harassed by a stalker in a foreign country who *inter alia* created and posted a false profile of her, as well as taunted, harassed and threatened her. Her teenage peers continued to taunt and ridicule her, face to face, online and in school and the community.

95 'The Facts about Online Hate and Cyberviolence', Canadian Women's Foundation, https://canadianwomen.org/the-facts/online-hate-and-cyberviolence.

96 'Cyberstalking in Canada', Statistics Canada, https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2017039-eng.htm.

97 'The Facts about Online Hate and Cyberviolence', Canadian Women's Foundation, https://canadianwomen.org/the-facts/online-hate-and-cyberviolence.

98 Ibid.

99 'Cyber Bullying Caribbean Culture', *Caribbean Goldstar* (2018), p. 1 https://caribbeanblackgoldstar.wordpress.com/2018/10/05/cyber-bullying-caribbean-culture/.

100 Ibid. See also: Sharana Mohamed (2017), 'Bullying among Students in Princes Town West Secondary', CAPE Caribbean Studies IA, which found similar impacts regarding self-esteem, depression and an inability to socialise in verbal and physical bullying among secondary students. available at https://www.slideshare.net/Zara_Mohammed/caribbeanstudies-ia-71974897

101 Canadian Parliamentary Committee, p. 36. See also LEAF, p. 29; and 'Cyberbullying and Youth', *Trinidad and Tobago Guardian* (2015), p. 2, https://www.guardian.co.tt/article-6.2.376401.37bb05bd92.

102 'Facts on Bullying and Harassment', Canadian Red Cross, https://www.redcross.ca/how-we-help/violence-bullying-and-abuse-prevention/educators/bullying-and-harassment-prevention/facts-on-bullying-and-harassment.

103 Chantalle A. Cummings (2017), 'I Can't See You, You Can't See Me: Cyberbullying – An Exploratory Study Examining This Concept through the Lens of the Social Bond Theory', *International Journal of Criminal and Forensic Science* Vol. 1 No. 2, 32–40,

104 Ibid., pp. 36–37.

105 LEAF, p. 25. See also: 'The Facts about Online Hate and Cyberviolence', Canadian Women's Foundation, https://canadianwomen.org/the-facts/online-hate-and-cyberviolence.

106 LEAF, pp. 36–37.

107 Ibid. And see: 'Facts and Figures: Ending Violence against Women', UN Women (March 2021), https://www.unwomen.org/en/what-we-do/endng-violence/facts-and-figures, citing Inter-Parliamentary Union, 'Sexism, Harassment and Violence against Women Parliamentarians', United Nations IPU Archive (October 2016), http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf.

108 LEAF, p. 37.

109 LEAF, pp. 38–39.

110 LEAF, p. 39.

111 LEAF, p. 26, and pp. 37–38.

112 'The Facts about Online Hate and Cyberviolence', Canadian Women's Foundation, https://canadianwomen.org/the-facts/online-hate-and-cyberviolence.

113 Ibid.

114 LEAF, p. 28.

115 'Caribbean Community Organizations Call for Decisive Action to End Homophobic Abuse and Cyberbullying', UNAIDS (2020), https://www.unaids.org/en/resources/presscentre/featurestories/2020/may/20200529_caribbean_homophobia_bullying.

116 LEAF, p. 19, and also pp. 3 and 16.

117 Canadian Parliamentary Committee, p. 40.

118 Canadian Parliamentary Committee, pp. 39–40.

119 Angela Hudson-Davis et al., 'The Psychology of the Bullying Phenomenon in Three Jamaican Public Primary Schools: A Need for a Public Health Trust', *International Journal of Emergency Mental Health & Human Resilience*, 17(2) (2017), p. 407, cited in 'Cyber Bullying Caribbean Culture' *Caribbean Goldstar* (2018), p. 2, https://caribbeanblackgoldstar.wordpress.com/2018/10/05/cyber-bullying-caribbean-culture/.

120 Nicoleta Metri, 'Building Awareness of Digital Violence against Barbadian Women', *Internet Society* (26 July 2018), https://www.internetsociety.org/blog/2018/07/building-awareness-of-digital-violence-against-barbadian-women/.

121 E. Shultz, R. Heilman and K. J. Hart, 'Cyber-bullying: An Exploration of Bystander Behavior and Motivation', *Cyberpsychology: Journal of*

Psychosocial Research on Cyberspace, 8(4) (2014), article 3, https://doi.org/10.5817/CP2014-4-3.

122 Megan M. Armstrong, 'An Exploratory Examination of the Bystander Effect in Cyberbullying', https://scholarworks.unr.edu/bitstream/handle/11714/2551/Armstrong_unr_0139D_11839.pdf?sequence=1&isAllowed=y.

123 Goran Sluiter, 'Aiding and Abetting Liability for Social Media Platforms in Relation to Image-based Sexual Abuse – a Way around Article 14 (1) of EU Directive 2000/31?', Rethinking SLIC (2021), https://rethinkingslic.org/blog/criminal-law/102-goeran-sluiter. Vikram Jeet Singh and Prashant Mara, 'Liable vs. Accountable: How Criminal Use of Online Platforms and Social Media Poses Challenges to Intermediary Protection in India – Media, Telecoms, IT, Entertainment', Mondaq.com (2020), https://www.mondaq.com/india/social-media/928106/liable-vs-accountable-how-criminal-use-of-online-platforms-and-social-media-poses-challenges-to-intermediary-protection-in-india.

124 R.S.C. 1985, c. C-46, as amended, https://laws-lois.justice.gc.ca/eng/acts/c-46/ (hereinafter referred to as 'Canada, Criminal Code').

125 David Watt and Michelle Fuerst, *Tremeear's Criminal Code*, annotated, Thomson Reuters (2021), commentary at pp. 74 and 78.

126 Ibid.

127 *Penal Code*, c. 84, Statute Law of the Bahamas, s. 86, http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1873/1873-0015/PenalCode_1.pdf (hereinafter 'Bahamas, Penal Code').

128 Ibid.

129 E.g., The Bahamas, Computer Misuse, 2006, c. 107A, s. 10, http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf; Belize, Cybercrime Act, 2020, https://www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf; Guyana, Cybercrime Act, 2018, s. 22, https://parliament.gov.gy/publications/acts-of-parliament/cyber-crime-act-2018; and Jamaica, The Cybercrimes Act, 2015 s. 12, https://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf.

130 E.g., Canada, Criminal Code, s. 264 (criminal harassment).

131 E.g., Canada, Criminal Code, s. 372 (false messages, indecent or harassing telephone calls).

132 Canada, Criminal Code, s. 163.

133 Canada, Criminal Code, s. 162.1 (publication, etc., of an intimate image without consent) .

134 Canada, Criminal Code, s. 162.2 (prohibition order).

135 Canada, Criminal Code, s. 162 (voyeurism).

136 Antigua and Barbuda, Electronic Crimes (Amendment) Act of 2018, s. 8 (violation of privacy), http://laws.gov.ag/wp-content/uploads/2019/02/No.-25-of-2018-Electronic-Crimes-Amendment-Act-2018.pdf; and Grenada, Electronic Crimes Act, 2013, s. 10 (violation of privacy), https://nowgrenada.com/wp-content/uploads/2013/07/Electronic-Crimes-Bill.pdf?x65460.

137 Saint Vincent and Grenadines, Cybercrime Act, 2016, s. 15 (violation of privacy) and s. 16 (sexual harassment by electronic communication), http://assembly.gov.vc/assembly/images/ActsBillsPolicies/SVG_Cybercrime_Act_2016.pdf.

138 Guyana, Cybercrime Act, 2018, s. 16 (publication or transmission of image of private area of a person), and ss. 39–41 (forfeiture, compensation), https://parliament.gov.gy/publications/acts-of-parliament/cyber-crime-act-2018.

139 Belize, Cybercrime Act, 2020, s. 12, s. 33, https://www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf.

140 St Vincent and Grenadines, s. 17.

141 St Vincent and Grenadines, s. 18.

142 E.g., 'St Vincent and Grenadines Adopts Cybercrime Law', *Newsroom* (2016), https://ipi.media/st-vincent-and-grenadines-

adopts-cybercrime-law/; 'New Cybercrime Law is Fundamentally Flawed', IFEX (2016), https://ifex.org/new-cybercrime-law-is-fundamentally-flawed/; 'St Vincent and the Grenadines Law Would Allow Prison for Defamation Online', UNHCR (2016), https://www.refworld.org/docid/57b2d22415.html.

143 Barbados, Computer Misuse, 2005, s. 14 (malicious communications), http://104.238.85.55/en/ShowPdf/124B.pdf; and Jamaica, The Cybercrimes Act, 2015, s. 9 (use of computer for malicious communication), https://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf.

144 St Kitts and Nevis, Electronic Crimes Act, 2009, s. 14 (unlawful communications), https://www.oas.org/juridico/spanish/cyber/questVII_kitts.pdf; and see Electronic Crimes (Amendment) Bill, 2012, s. 11, http://www.sknlist.com/20120614a.html.

145 Saint Lucia, Electronic Crimes Act, 2009, s. 7 (cyber stalking), http://www.govt.lc/media.govt.lc/www/resources/legislation/ElectronicCrimesBill.pdf; http://www.govt.lc/legislation/electronic-crimes-bill; and Grenada, Grenada, Electronic Crimes Act of 2013, s. 6 and s. 16.

146 Antigua and Barbuda, Electronic Crimes Act, 2013, s. 13, http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf.

147 Grenada, Electronic Crimes Act, 2013, s. 6 and s. 16, https://nowgrenada.com/wp-content/uploads/2013/07/Electronic-Crimes-Bill.pdf?x65460; Antigua and Barbuda, Electronic Crimes Act, 2013, s. 4, http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf.

148 'Grenada Parliament Amends Electronic Defamation Law', International Press Institute (12 March 2014), https://ipi.media/grenada-parliament-amends-electronic-defamation-law/; Grenada, Electronic Crimes (Amendment) Act, 2014, www.gov.gd/sites/hop/files/Acts-SROs/2014/Act%20No.%2010%20of%202014%20Electronic%20Crimes%20(Amendment).pdf; and Antigua and Barbuda, Electronic Crimes (Amendment) Act, 2018, s. 4, http://laws.gov.ag/wp-content/uploads/2019/02/No.-25-of-2018-Electronic-Crimes-Amendment-Act-2018.pdf.

149 Guyana, Cybercrime Act, 2018, s. 19, https://parliament.gov.gy/publications/acts-of-parliament/cyber-crime-act-2018; Belize, Cybercrime Act, 2020, s. 15, https://www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf.

150 British Virgin Islands, Computer Misuse and Cybercrime (Amendment) Act, 2019, s. 7 enacting new ss. 14A and 14B, https://centre.caribbeancspa.org/hc/en-gb/sections/360005122379-Caribbean-Cyber-Crime-Laws.

151 'New Cybercrime Bill Threatens Press Freedom in British Virgin Islands', International Press Institute (3 December 2019), https://ipi.media/new-cybercrime-bill-threatens-press-freedom-inbritsh-virgin-islands/; 'British Virgin Islands Law to Impose Fine, Jail Terms for Online Defamation', Committee to Protect Journalists (23 December 2019), https://cpj.org/2019/12/british-virgin-islands-law-to-impose-fines-jail-te/; 'Statement by Governor Jaspert on the Computer Misuse and Cybercrime Amendment Act, 2019', Government of the Virgin Islands (12 February 2020), http://www.bvi.gov.vg/media-centre/statement-governor-jaspert-computer-misuse-and-cybercrime-amendment-act-2019.

152 Bill 15 to enact the 'Cybercrime Act, 2017', 2nd Session, 11th Parliament Republic of Trinidad and Tobago, proposed ss. 18 and 16, http://www.ttparliament.org/legislations/b2017h15g.pdf.

153 St Kitts and Nevis, Electronic Crimes Act, 2009, s. 14(2) (unlawful communications), https://www.oas.org/juridico/spanish/cyber/questVII_kitts.pdf; and see Electronic Crimes (Amendment) Bill, 2012, s. 11, http://www.sknlist.com/20120614a.html.

154 E.g., Antigua and Barbuda, The Bahamas, Barbados, Dominica, Grenada, Jamaica, Saint Lucia, St Vincent and Grenadines, Trinidad and Tobago, and British Virgin Islands (UK).

155 E.g., Grenada, Electronic Crimes Act, 2013, s. 6 and s. 16, which have been amended/repealed in 2014; St Vincent and Grenadines, Cybercrime Act, 2016, s. 19, http://assembly.gov.vc/assembly/images/ActsBillsPolicies/SVG_Cybercrime_Act_2016.pdf; and Antigua and Barbuda, Electronic Crimes (Amendment) Act, 2018, s. 4, http://laws.gov.ag/wp-content/uploads/2019/02/No.-25-of-2018-Electronic-Crimes-Amendment-Act-2018.pdf, as discussed above. Grenada amended its electronic defamation law to address some criticisms, 'Grenada Parliament Amends Electronic Defamation Law', International Press Institute (12 March 2014), https://ipi.media/grenada-parliament-amends-electronic-defamation-law/. See also criticism of British Virgin Islands, Computer Misuse and Cybercrime (Amendment) Act, 2019, which was eventually brought into effect without amendment. See discussion and footnotes, above, referring to British Virgin Islands.

156 For an analysis of criminal defamation and libel laws in the Caribbean, including their application to the Internet, see: 'Criminal Defamation Laws in the Caribbean', Committee to Protect Journalists (2016), https://cpj.org/reports/2016/03/the-caribbean/.

157 Canada, Criminal Code, s. 298–301. (defamatory libel).

158 *E.g., R. v. Lucas*, [1998] 1 S.C.R. 14; *R. v. Gill* (1996), 29 O.R. (3d) 250 (Gen Div.); *R. v. Prior* (2008), 231 C.C.C. (3d) 12, 57 C.R. (6th) 387 (N.L. T.D).

159 British Virgin Islands, Computer Misuse and Cybercrime (Amendment) Act, 2019, s. 7 enacting new ss. 14A and 14B, https://centre.caribbeancspa.org/hc/en-gb/sections/360005122379-Caribbean-Cyber-Crime-Laws.

160 E.g., Canada, Criminal Code, s. 264.1 (uttering threats).

161 E.g., Canada, Criminal Code, s. 423 (intimidation), which applies in both the offline and online realms; Guyana, s. 19; and Belize, s. 15 (use of a computer to coerce, harass, intimidate or humiliate), which is limited to the online realm.

162 E.g., Canada, Criminal Code, s. 184 (interception of private communication); Jamaica, The Interception of Communications (Amendment) Act (2011), http://laws.moj.gov.jm/.

163 In this regard, the enactment in jurisdictions of criminal offences, which are aligned with the Commonwealth Model Law on Computer and Computer Related Crime, is an important tool to address some forms of cyberviolence: e.g., Antigua and Barbuda, Electronic Crimes Act of 2013, s. 3, http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf, and Electronic Crimes (Amendment) Act of 2018, s. 4, http://laws.gov.ag/wp-content/uploads/2019/02/No.-25-of-2018-Electronic-Crimes-Amendment-Act-2018.pdf; The Bahamas, Computer Misuse Act, Act No. 2 of 2003; Barbados, Computer Misuse Act (2005), ss. 4, 6 and 7, http://www.oas.org/juridico/spanish/cyb_bbs_computer_misuse_2005.pdf; Belize, Cybercrime Act, 2020, https://www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf; Bermuda, Computer Misuse Act, 1996, ss. 3 and 4, http://www.bermudalaws.bm/laws/Consolidated%20Laws/Computer%20Misuse%20Act%201996.pdf; Grenada, Electronic Crimes Act, 2013, ss. 3–5, https://nowgrenada.com/wp-content/uploads/2013/07/Electronic-Crimes-Bill.pdf?x65460Guyana; Guyana, Cybercrime Act, 2018, ss. 3, 4 and 9, https://parliament.gov.gy/publications/acts-of-parliament/cyber-crime-act-2018; Jamaica, The Cybercrimes Act, 2015, https://www.japarliament.gov.jm/attachments/339_The%20Cybercrimes%20Acts,%202015.pdf and The Cybercrimes Act, 2010, https://moj.gov.jm/sites/default/files/laws/Cybercrimes%20Act.pdf; St Kitts and Nevis, ss. 4, 6 and 7, https://www.oas.org/juridico/spanish/cyber/questVII_kitts.pdf, and as amended in 2012, http://www.sknlist.com/20120614a.html; Saint Lucia, Electronic Crimes Act, 2009, ss. 5 and 6, http://www.govt.lc/media.govt.lc/www/resources/legislation/ElectronicCrimesBill.pdf; Saint Vincent and Grenadines, Cybercrime Act 2016, Cybercrime Act 2016, ss. 3, 5 and 7, http://assembly.gov.vc/assembly/images/ActsBillsPolicies/SVG_Cybercrime_Act_2016.pdf; Trinidad

and Tobago, Computer Misuse Act (2000), ss. 3, 4 and 6, https://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/11.17.pdf; British Virgin Islands, Computer Misuse and Cybercrime (Amendment) Act, 2019, https://centre.caribbeancspa.org/hc/en-gb/sections/360005122379-Caribbean-Cyber-Crime-Laws; and Canada, Criminal Code, R.S.C. 1985, c. C-46, as amended, s. 342.1 (unauthorised use of computer systems), https://laws-lois.justice.gc.ca/eng/acts/c-46/.

164 E.g., Criminal Code, s. 162 (voyeurism), which applies in both the offline and online realms. See also Trinidad and Tobago, Bill 15 to enact 'Cybercrime Act, 2017', s. 16, https://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/11.17.pdf.

165 E.g., The Bahamas, Penal Code, s. 368 and s. 370 (forgery); Canada, Criminal Code, s. 366 (forgery), which apply in both offline and online realms. Some jurisdictions have enacted specific electronic forgery laws in their computer crime statutes: e.g., Antigua and Barbuda Electronic Crimes (Amendment) Bill 2018, s. 6; Belize Cybercrime Act 2020 s. 8; Grenada Electronic Crimes Act 2013, s. 8; Guyana Cybercrime Act 2018, s. 10; Jamaica Computer Crimes Act 2015 s.8, Saint Lucia Electronic Crimes Bill, s. 11; and St Vincent and Grenadines Cybercrime Act 2016, s. 12.

166 E.g., The Bahamas, Penal Code, ss. 59, 60 and 348 (fraud by false pretence, personation); Canada, Criminal Code, s. 380 (fraud), which apply in both offline and online realms. Some jurisdictions have enacted specific electronic fraud laws in their computer crime statutes: e.g., Antigua and Barbuda, s. 7; Belize, s. 9; Grenada, s. 9; Guyana, s. 11; Jamaica, s. 8; St Kitts and Nevis, s. 9; and Saint Lucia, s. 12.

167 E.g., Canada, Criminal Code, s. 402.2 (identity theft) and s. 403 (identity fraud), which applies to both offline and online realms. Some jurisdictions have enacted specific electronic identity theft/fraud laws in their computer crime statutes: e.g., Antigua and Barbuda, s. 5; Belize, ss. 9 and 10; Grenada, s. 7; Guyana, s. 13; Saint Kitts and Nevis, s. 16; and St Vincent and Grenadines, s. 11. See also Trinidad and Tobago, proposed Bill 15 to enact 'Cybercrime Act, 2017', s. 13. 14 and 15, https://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/11.17.pdf.

168 E.g., The Bahamas, Penal Code, s. 346 (extortion); Canada, Criminal Code, s. 346 (extortion) and s. 302 (extortion by libel). See also: Trinidad and Tobago, Bill 15 to enact 'Cybercrime Act, 2017', s. 19, https://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/11.17.pdf.

169 E.g., Canada, Criminal Code, s. 423 (intimidation); Guyana, s. 19 (coerce, harass, intimidate, extort); and Belize, s. 15 (coerce, harass, intimidate, extort).

170 E.g., Canada, Criminal Code, s. 163.1 (child pornography), s. 153 (sexual exploitation), s. 172 (corrupting children), s. 172.1 (luring a child), s. 171.1 (making sexually explicit material to child), s. 172.2 (agreement or arrangement – sexual offence against child), s. 151 (sexual interference), s. 152 (invitation to sexual touching), s. 153.1 (sexual exploitation of person with disability), s. 286.1 (obtaining sexual service for consideration) and s. 163 (obscene materials). Special jurisdictional and procedural provisions also exist, such as s. 7(4.1) and (4.3) (offence in relation to sexual offences against children committed outside Canada deemed to have been committed in Canada), s. 164 and s. 164.1 (warrant of seizure), s. 164.2 (forfeiture after conviction) and s. 738(1) (restitution to victims of offences).

171 E.g., ibid., Canada's general offences regarding child pornography and sexual exploitation meet the model law requirements. Some Caribbean jurisdictions have specific computer crime laws regarding child pornography, or child luring, in their computer crime statutes: e.g., Antigua and Barbuda, s. 10, Barbados, s. 13; Belize, s. 11; Grenada, s. 12; Guyana, ss. 14 and 15; St Kitts and Nevis, s. 13; Saint Lucia, s. 16; St Vincent and Grenadines, s. 14; and British Virgin Islands.

172 Canada, An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons Who Provide an Internet Service, S.C. 2011, c. 4, https://www.laws.justice.gc.ca/eng/acts/I-20.7/index.html.

173 E.g., Canada, Criminal Code, s. 319, which includes identifiable groups distinguished by 'colour, race, religion, national or ethnic origin, age, sex, sexual orientation, gender identity or expression, or mental or physical disability'.

174 E.g., The Bahamas, Penal Code, s. 315; and see discussion above concerning criminal, computer defamation and libel (Section 5.1.1).

175 E.g., Canada, Criminal Code, s. 264.1 (uttering threats) and s. 264 (criminal harassment). Caribbean jurisdictions may have various statutes to address these types of threats against a person.

176 E.g., The Bahamas, Penal Code, s. 244 (making false report); Canada, Criminal Code, s. 140 (public mischief); and Grenada, Electronic Crimes Act of 2013, s. 15 (prank calls to law enforcement).

177 See text and footnote 155 references, above, in relation to the discussion on 'interception of private communications and data' for a list and citations of statutes: e.g., Antigua and Barbuda, Electronic Crimes Act, 2013 and Electronic Crimes (Amendment) Act, 2018; Barbados, Computer Misuse Act, 2005; The Bahamas, Computer Misuse Act, 2006; Belize, Cybercrime Act, 2020 https://www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf; Bermuda, Computer Misuse Act, 1996; Grenada, Electronic Crimes Act, 2013, as amended in 2014; Guyana, Cybercrime Act, 2016; Jamaica, The Cybercrimes Act, 2015; St Kitts and Nevis, Electronic Crimes Act, 2009, and Electronic Crimes (Amendment) Act, 2012; Saint Lucia, Electronic Crimes Act, 2009; Saint Vincent and Grenadines, Cybercrime Act, 2016; Trinidad and Tobago, Computer Misuse Act, 2000; and Canada, Criminal Code, s. 342.1 (unauthorized use of computer systems) and s. 430 (1.1) (mischief in relation to data). United Kingdom overseas territories: Cayman, Computer Misuse Law, 2015, https://www.ofreg.ky/upimages/commonfiles/1506773086ComputerMisuseLaw2015Revision.PDF; British Virgin Islands, Computer Misuse and Cybercrime (Amendment) Act, 2019, https://centre.caribbeancspa.org/hc/en-gb/sections/360005122379-Caribbean-Cyber-Crime-Laws.

178 'Report on the Regional Conference on Cybercrime Strategies and Policies and Features of the Budapest Convention for the Caribbean Community', Global Action on Cybercrime Extended (GLACY+), 2019, https://rm.coe.int/3148-1-1-3-final-report-dr-reg-conference-cy-policies-caribbean-comm-1/168098fb6c.

179 *Thompson v. Cohodes*, 2017 ONSC 2590.

180 *AB v. Bragg*, 2012 SCC 46.

181 *Jane Doe 72511 v. NM*, 2018 ONSC 6607, paras 59–96.

182 Ibid., para. 93.

183 *Caplan v. Atas*, 2021 ONSC 670, para 171.

184 Under the Canadian Constitution, the enactment of criminal law and procedure is within the exclusive jurisdiction of the federal Parliament and includes indictable and summary conviction offences. However, provincial legislatures may enact penal penalties to enforce their laws, which are proceeded by way of summary conviction procedures and maximum penalties are generally not more than two years of incarceration in a provincial penal institution. They may also administer and enforce federally enacted criminal laws and procedures. See: Constitution Act 1982, Canada Act 1982 (UK), c. 11 R.S.C. 1985, App. II No. 44, am., s. 91(27) and s. 92(14).

185 Intimate Images and Cyber-protection Act, SNS 2017, c 7 (Nova Scotia); The Privacy Act, RSS 1978, c P-24 (Saskatchewan); Intimate Image Protection Act, CCSM c 187 (Manitoba); Protecting Victims of Non-consensual Distribution of Intimate Images Act, RSA 2017, c P-26.9 (Alberta); Intimate Images Protection Act, RSPEI 1988, c I-9.1 (Prince Edward Island); Intimate Images Protection Act, RSNL 2018, c I-22 (Newfoundland and Labrador).

186 See for example, Intimate Images and Cyber-protection Act, SNS 2017, c 7, s. 6 (Nova Scotia).

187 Ibid.

188 Education Act, RSO 1990, c. E.2 – Ontario.ca, see Part XIII (Ontario); An Act to Prevent and Stop Bullying and Violence in Schools,

SQ 2012, c 19 (Quebec); Education Act, SA, 2012, c E-0.3, as am. (Alberta); Education Act, SNB 1997, c E-1.12, as am. (New Brunswick); The Cyberbullying Prevention Act, SM 2013, 40th Legislature, 2nd Session (Manitoba); and Education Act, SNWT (Nu) 1995, c25, as am. (Northwest Territories).

189 Ibid., Alberta.

190 Ibid., Manitoba.

191 E.g., Antigua and Barbuda, ss. 29 and 30; The Bahamas, ss. 12 and 17; Barbados, s. 21; Bermuda, s. 12; Grenada, ss. 31 and 32; Guyana, ss. 39–41; Jamaica, ss. 15 and 20; Saint Lucia, ss. 33 and 34; St Vincent and Grenadines, ss. 31 and 32; and UK: Cayman Islands, s. 14.

192 Cynthia Khoo, 'Deplatforming Misoggny: Report on Platform Liability for Technology-facilitated Gender-based Violence', Women's Legal Education and Action Fund (LEAF) (April 2021), https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf, see chapter 4. Platform Liability for TFGBV in Canadian, Law, pp. 97–132.

193 St Vincent and the Grenadines, Cybercrime Act, 2016, ss. 40–45, http://assembly.gov.vc/assembly/images/ActsBillsPolicies/SVG_Cybercrime_Act_2016.pdf.

194 Belize Cybercrime Act 2020, s. 13, https://www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf.

195 Ibid.

196 Canadian Parliamentary Committee (hate), p. 26; Canadian Parliamentary Committee (violence), pp. 51–52.

197 Canadian Parliamentary Committee (violence), pp. 53–54.

198 Ibid., pp. 27–28; pp. 51–52, respectively.

199 Ibid., pp. 28–30.

200 Council of Europe, pp. 18–21.

201 See also Canadian Parliamentary Committee, pp. 44–45.

202 Canadian Parliamentary Committee, p. 41.

203 Ibid., p. 39.

204 IACHR, p. 136.

205 Ibid., and see Section 4.

206 Canadian Parliamentary Committee, pp. 41–42.

207 Ibid. p. 39.

208 Ibid., p. 40.

209 'Annual Report of the Special Representative of the Secretary-General on Violence against Children', UN Human Rights Council, 31st session (2016), for a description of cyberbullying and its impact on children, https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Documents/A_HRC_31_20_E.doc.

210 Section x.x.

211 Canadian Parliamentary Committee, pp. 44–47.

212 Canadian Parliamentary Committee, pp. 44, 47.

213 Cybertip.ca (2022) 'Protecting Children Online', Canada's National Tipline for Reporting the Online Sexual Exploitation of Children, https://www.cybertip.ca/app/en/.

214 'An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons Who Provide an Internet Service', S.C. 2011, c. 4. https://laws.lois.justice.gc.ca/eng/acts.

215 Canadian Parliamentary Committee, p. 48.

216 Ibid., p. 49.

217 Ibid.

218 Ibid., pp. 49–50.

219 Ibid., p. 76.

220 Ibid.

221 'A Report to Guide the Implementation of a National Action Plan on Violence against Women and Gender-based Violence', Women's Shelters Canada (April 2021), https://www.nationalactionplan.ca/wp-content/uploads/2021/06/NAP-Final-Report.pdf.

222 IACHR, p. 135.

223 Ibid., p. 142.

224 'Taking Action to End Online Hate', Report of the Standing Committee on Justice and Human Rights, 42nd Parliament, 1st Session, June 2019 (Anthony Housefather, Chair).

225 Ibid., pp. 40–42.

226 Ibid., p. 42.

227 E.g., Matthew Baker, 'Cyberbullying and the Bystander: What Promotes or Inhibits Adolescent Participation?', University of Exeter (2014), https://ore.exeter.ac.uk/repository/bitstream/handle/10871/17324/BakerM.pdf?sequence=1&isAllowed=y; Warren Robin, 'Bullying, Victims, and Bystanders: From Prevalence to Prevention', University of Pennsylvania, https://www.academia.edu/2896809/Bullies_Victims_and_Bystanders_From_Prevalence_to_Prevention?email_work_card=reading-history.

228 'Survey Reveals One in Three Canadians Who Witness Cyber-bullying Stand up to It', Canadian Red Cross (2017), https://www.redcross.ca/about-us/media-news/news-releases/survey-reveals-one-in-three-canadians-who-witness-cyber-bullying-stand-up-to-it.

229 'Bystanders in Cyberbullying', McGill University (2018), p. 1, https://www.mcgill.ca/newsroom/channels/news/bystanders-cyberbullying-288182.

230 Ibid.

231 'Cyber Bullying Caribbean Culture', *Caribbean Goldstar* (2018), p. 2. https://caribbeanblackgoldstar.wordpress.com/2018/10/05/cyber-bullying-caribbean-culture/.

232 'Bystander Effect', *Psychology Today Canada*, pp. 1–3, https://www.psychologytoday.com/ca/basics/bystander-effect.

233 Taylor DiFranzo et al., 'Upstanding by Design: Bystander Intervention in Cyberbullying', Cornell and Ithaca Universities, pp. 7 and 9, https://cpb-us-e1.wpmucdn.com/blogs.cornell.edu/dist/c/6136/files/2013/12/Upstanding-by-Design-2c0ielg.pdf.

234 E.g., 'Bystander Intervention Strategies', Government of Canada, https://www.canada.ca/en/department-national-defence/services/benefits-military/conflict-misconduct/operation-honour/training-educational-materials/bystander-intervention-strategies.html.

235 E.g., Ann-Lee Straatman, 'Bystander Sexual Violence Education Programs for High School, College and University Students', Learning Network Brief (09), London, Ontario, Learning Network, Centre for Research and Education on Violence Against Women and Children, http://www.vawlearningnetwork.ca/; 'Bystander Intervention', University of Victoria (BC), https://www.uvic.ca/services/studentlife/initiatives/bystander-intervention/.

236 N. Naffi, 'Don't Be a Bystander: Five Steps to Fight Cyberbullying', Concordia University, https://theconversation.com/dont-be-a-bystander-five-steps-to-fight-cyberbullying-91440.

237 Daveny Ellis, 'How to: 6 Ways to Deal with Cyberbullying and Online Harassment', *Loop News*, https://barbados.loopnews.com/content/how-deal-cyberbullies.

238 'Get Safe Online! Avoid Cyberstalking', Caribbean Union Adventists (2021), https://www.caribbeanunionadventists.org/news/features/info/get-safe-online-avoid-cyberstalking.

239 'International Day against Violence and Bullying at School Including Cyberbullying', UNESCO (2020), https://en.unesco.org/commemorations/dayagainstschoolviolenceandbullying.

240 'Alarming Figures of Bullying in Latin America and the Caribbean', *LatinAmerican Post* (2018), p. 5, https://latinamericanpost.com/24051-the-alarming-figures-of-bullying-in-latin-america-and-the-caribbean; Nicoletta Metri, 'Building Awareness of Digital Violence against Barbadian Women', *Internet Society* (26 July 2018), https://www.internetsociety.org/blog/2018/07/building-awareness-of-digital-violence-against-barbadian-women/.

241 'Survey Reveals One in Three Canadians Who Witness Cyber-bullying Stand up to It', Canadian Red Cross (2017), https://www.redcross.ca/about-us/media-news/news-releases/survey-reveals-one-in-three-canadians-who-witness-cyber-bullying-stand-up-to-it; 'Cyberbullying and Youth, Part Two', *Trinidad and Tobago Guardian* (2015), pp. 1–2, https://www.guardian.co.tt/article-6.2.361986.53e547c651; Hodine Williams and Andrae Campbell, 'A Punch at Cyber Bullying', *Jamaica Observer* (2016), pp. 1–6, https://www.jamaicaobserver.com/news/a-punch-at-cyber-bullying_78983.

242 Royal Canadian Mounted Police: 'Delete Cyberbullying', https://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/video/cyber-video-eng.htm; 'Bullying', https://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/pdf/bully-int-eng.pdf; 'Online Safety – Learning Resources', https://www.rcmp-grc.gc.ca/cycp-cpcj/is-si/isres-ressi-eng.htm.

243 info@caribbeansecurityinstitute.com or www.caribbeansecurityinstitute.com.

244 'Life in Leggings: Caribbean Alliance against Gender-based Violence', (Barbados, 29 August 2019 post), https://www.facebook.com/officiallifeinleggings/, or *Barbados Today* (24 August 2019), https://barbadostoday.bb/2019/08/24/cyber-crime-watch/.

245 'Government of Canada Awareness Campaign Addresses Growing Risk of Online Child Sexual Exploitation', Public Safety Canada (12 July 2021), https://www.canada.ca/en/public-safety-canada/news/2021/07/government-of-canada-awareness-campaign-addresses-growing-risk-of-online-child-sexual-exploitation.html.

246 See Section 5.

247 'Cyberbullying and Non-consensual Distribution of Intimate Images: CCSO Cybercrime Working Group, Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety' (June 2013), https://www.justice.gc.ca/eng/rp-pr/other-autre/cndii/p6.html. The Canadian statutes are based primarily on the philosophical underpinning that the unlawful conduct is a violation of privacy.

248 Bill to enact the 'Cybercrime Act, 2017', 2nd Session, 11th Parliament, Republic of Trinidad and Tobago, proposed s. 18, http://www.ttparliament.org/legislations/b2017h15g.pdf (hereinafter 'T&T cybercrime proposals').

249 'RSF Concerned by Certain Provisions of Trinidad and Tobago's Cybercrime Bill', Reporters Without Borders (9 May 2017), https://rsf.org/en/news/rsf-concerned-certain-provisions-trinidad-and-tobagos-cybercrime-bill.

250 Ibid., proposed s. 16. Some other criticisms of the bill have been raised; e.g., 'Public Comment on the Trinidad and Tobago CyberCrime Bill, 2017', KnowProSE.com (13 June 2017), https://knowprose.com/2017/06/13/public-comment-on-the-trinidad-and-tobago-cybercrime-bill-2017/.

251 'Cybecrime/E-crimes: Model Policy Guidelines and Legislative Texts', HIPCAR (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean), s. 18, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf (hereinafter, 'HIPCAR cybercrime proposals').

252 While computer systems are used to operate telecommunication services and networks, these services and networks (e.g., telephone services) may not necessarily be considered to be computer systems, see: *R. v. McLaughlin*, [1980] 2 S.C.R. 331 (Canada).

253 Canada, Criminal Code, s. 264 (criminal harassment), s. 423 (intimidation), s. 264.1 (uttering threats), s. 346 (extortion), s. 162 (voyeurism) and s. 162.1 (publication, etc., of an intimate image without consent).

254 Trinidad & Tobago Cybercrime Bill 2017, ss. 15 and 13; HIPCAR cybercrime proposals, ss. 14 and 11.

255 Trinidad &Tobago Cybercrime Bill 2017, s. 8.

256 'Will Trinidad and Tobago's Cybercrime Bill Stifle Media Freedom?', IFEX (29 June 2018), https://ifex.org/will-trinidad-and-tobagos-cybercrime-bill-stifle-media-freedom/; and 'RSF Concerned by Certain Provisions of Trinidad and Tobago's Cybercrime Bill', Reporters Without Borders (9

May 2017) https://rsf.org/en/news/rsf-concerned-certain-provisions-trinidad-and-tobagos-cybercrime-bill.

257 HIPCAR cybercrime proposals, ss. 4 and 6.

258 Trinidad and Tobago Cybercrime Bill 2017, s. 19.

259 HIPCAR cybercrime proposals, s. 13.

260 'Report on the Regional Conference on Cybercrime Strategies and Policies and Features of the Budapest Convention for the Caribbean Community', Global Action on Cybercrime Extended (GLACY+), 2019, https://rm.coe.int/3148-1-1-3-final-report-dr-reg-conference-cy-policies-caribbean-comm-1/168098fb6c.

261 Bill C-36, 'An Act to Amend the Criminal Code and the Canadian Human Rights Act and to Make Related Amendments to Another Act (Hate Propaganda, Hate Crimes and Hate Speech)', 43rd Parliament, 2nd Session, 69–70 Elizabeth II, 2020–2021 (First Reading, 23 June 2021), https://parl.ca/DocumentViewer/en/43-2/bill/C-36/first-reading#IDOE3AA.

262 'Creating a Safe, Inclusive and Open Online Environment', Canadian Heritage (29 July 2021), https://www.canada.ca/en/canadian-heritage/news/2021/07/creating-a-safe--inclusive-and-open-online-environment.html.

263 'Discussion Guide', Canadian Heritage (29 July 2021), https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html.

264 Ibid., pp. 6–8.

265 Ibid., pp. 8–10 and 14–16.

266 Ibid., pp. 13–15.

267 Ibid., pp. 10–12.

268 The Uniform Law Conference of Canada (ULCC) is an organisation, funded primarily by the federal and provincial/territorial governments, and composed of representatives of government, academia, private practice and law reform commissions, with a mandate to develop model laws and other documents to address gaps or jurisdictional inconsistencies in various areas of criminal and civil law, including modernisation and greater harmonisation or alignment of legal approaches across provinces and territories. See: Uniform Law Conference of Canada, 'What We Do' (2019), https://www.ulcc.ca/en/about-us-en-gb-1/what-we-do.

269 Uniform Law Conference of Canada, 'Uniform Non-consensual Disclosure of Intimate Images Act: Report of the Working Group and Draft Uniform Act', https://www.ulcc-chlc.ca/ULCC/media/EN-Annual-Meeting-2020/Report-of-the-Working-Group-and-Draft-Uniform-Act-2020.pdf (hereinafter 'ULCC Uniform Act'). The report and draft uniform Act were significantly influenced by a paper by Hilary Young and Emily Laidlaw, 'Creating a Revenge Porn Tort for Canada', *Supreme Court Law Review* 147 (2020).

270 ULCC Uniform Act, s. 3: 'A person who distributes or threatens to distribute an intimate image commits a tort that is actionable without proof of damage'

271 ULCC Uniform Act, s. 3 and 4; and see commentary at pp. 1, 2, 5 and 10–13.

272 ULCC Uniform Act, ss. 3 and 5; and see commentary at pp. 1, 2, 5 and 13–16.

273 Ibid., pp. 8–9.

274 Ibid., s. 1; and see commentary at pp. 3 and 9.

275 Ibid., s. 1; and see commentary at pp. 7–8.

276 Ibid., p. 9.

277 Ibid., s. 6, and see commentary at p. 15.

278 Ibid., s. 7, and see commentary at pp. 15–16.

279 Ibid., s. 9, and see commentary pp. 16–17.

280 Ibid., s. 10, and see commentary p. 17.

281 Ibid., pp. 17–18.

282 Ibid., s. 11, see commentary at pp. 18–19.

283 Ibid. s. 1 and s. 8, see commentary at pp. 7 and 16.

284 LEAF, p. 125.

285 'Defamation Law in the Internet Age', Law Commission of Ontario (March 2020), https://www.lco-cdo.org/en/our-current-projects/defamation-law-in-the-internet-age/ (hereinafter 'LCO report').

286 Ibid., See Executive Summary, pp. 3–4, https://www.lco-cdo.org/wp-content/uploads/2020/03/Defamation-Executive-Summary-Eng-FINAL.pdf (hereinafter 'LCO Executive Summary').

287 LCO Executive Summary, p. 5.

288 Ibid., p. 9.

289 LCO report, p. 84.

290 LCO Executive Summary, p. 11.

291 Ibid.

292 LEAF, p. 127.

293 LEAF, pp. 127–128.

Bibliography

Armstrong, MM (2015). 'An Exploratory Examination of the Bystander Effect in Cyberbullying', University of Nevada, available at: https://scholarworks.unr.edu/bitstream/handle/11714/2551/Armstrong_unr_0139D_11839.pdf?sequence=1&isAllowed=y.

Bailey, J, V Steeves and S Dunn (2017). 'Submission to the Special Rapporteur on Violence Against Women re: Regulating Online Violence and Harassment against Women', *eQuality Project*, University of Ottawa, available at: http://www.equalityproject.ca/wp-content/uploads/2017/12/Bailey-Steeves-Dunn-Submission-27-Sep-2017.pdf.

Baker, M (2014). 'Cyberbullying and the Bystander: What Promotes or Inhibits Adolescent Participation?' University of Exeter, available at: https://ore.exeter.ac.uk/repository/bitstream/handle/10871/17324/BakerM.pdf?sequence=1&isAllowed=y.

Barbados Today (2019). 'Cyber Crime Watch', available at: https://barbadostoday.bb/2019/08/24/cyber-crime-watch/.

Best, G (2017). 'Caribbean Girls under Cyber Attack', *Silcon Caribe*, available at: https://www.siliconcaribe.com/2017/05/04/caribbean-girls-under-cyber-attack/.

Canadian Heritage, Government of Canada (2021). 'Creating a Safe, Inclusive and Open Online Environment', available at: https://www.canada.ca/en/canadian-heritage/news/2021/07/creating-a-safe-inclusive-and-open-online-environment.html.

Canadian Heritage, Government of Canada (2021). 'Discussion Guide', available at: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html.

Canadian Red Cross (2022). 'Facts on Bullying and Harassment', available at: https://www.redcross.ca/how-we-help/violence-bullying-and-abuse-prevention/educators/bullying-and-harassment-prevention/facts-on-bullying-and-harassment.

Canadian Red Cross (2017). 'Survey Reveals One in Three Canadians Who Witness Cyber-bullying Stand up to It', available at: https://www.redcross.ca/about-us/media-news/news-releases/survey-reveals-one-in-three-canadians-who-witness-cyber-bullying-stand-up-to-it.

Canadian Women's Foundation (2019). 'The Facts about Online Hate and Cyberviolence', available at: https://canadianwomen.org/the-facts/online-hate-and-cyberviolence.

Caribbean Goldstar (2018). 'Cyber Bullying Caribbean Culture', available at: https://caribbeanblackgoldstar.wordpress.com/2018/10/05/cyber-bullying-caribbean-culture/.

Caribbean Institute for Security & Public Safety (CISPS). available at: info@caribbeansecurityinstitute.com , or www.caribbeansecurityinstitute.com.

Caribbean Union Adventists (2021). 'Get Safe Online! Avoid Cyberstalking', available at: https://www.caribbeanunionadventists.org/news/features/info/get-safe-online-avoid-cyberstalking.

Committee to Protect Journalists (2016). 'Criminal Defamation Laws in the Caribbean', available at: https://cpj.org/reports/2016/03/the-caribbean/.

Committee to Protect Journalists (2019). 'British Virgin Islands Law to Impose Fine, Jail Terms for Online Defamation', available at: https://cpj.org/2019/12/british-virgin-islands-law-to-impose-fines-jail-te/.

Commonwealth, The (2017). *Model Law on Computer and Computer Related Crime*, available at: https://www.thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf.

Council of Europe (2011). *Convention on Violence against Women and Domestic Violence (CETS 210)*. (Istanbul Convention). https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210.

Council of Europe (2018). Cybercrime Convention Committee, T-CY (2017)10 [EN] Mapping Study on Cyberviolence, [FR] Etude cartographique sur la cyberviolence, available at: www.coe.int/cybercrime.

Cummings, CA (2017). 'I Can't See You, You Can't See Me: Cyberbullying – An Exploratory Study Examining This Concept through the Lens of the Social Bond Theory', *International Journal of Criminal and Forensic Science* 1(2) (2017), 32–39.

Department of Justice, Government of Canada (2013). *Cyberbullying and Non-consensual Distribution of Intimate Images*, CCSO Cybercrime Working Group, Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety, available at: https://www.justice.gc.ca/eng/rp-pr/other-autre/cndii-cdncii/index.html.

Department of National Defence, Government of Canada (2021). 'Bystander Intervention Strategies', available at: https://www.canada.ca/en/department-national-defence/services/benefits-military/conflict- /operation-honour/training-educational-materials/bystander-intervention-strategies.html.

DiFranzo, T et al , (2018) 'Upstanding by Design: Bystander Intervention in Cyberbullying', Cornell and Ithaca Universities, available at: https://cpb-us-e1.wpmucdn.com/blogs.cornell.edu/dist/c/6136 / files/2013/12/Upstanding-by-Design-2c0ielg.pdf.

Ellis, D (2020). '6 Ways to Deal with Cyberbullying and Online Harassment', *Loop News*, available at: https://barbados.loopnews.com/content/how-deal-cyberbullies.

Global Action on Cybercrime Extended (GLACY+) (2019). *Report on the Regional Conference on Cybercrime Strategies and Policies and Features of the Budapest Convention for the Caribbean Community*, available at: https://rm.coe.int/3148–3141-1-3-final-report-dr-reg-conference-cy-policies-caribbean-comm-1/168098fb6c.

Government of the Virgin Islands (2020). 'Statement by Governor Jaspert on the Computer Misuse and Cybercrime Amendment Act, 2019', available at: http://www.bvi.gov.vg/media-centre/statement-governor-jaspert-computer-misuse-and-cybercrime-amendment-act-2019.

HG.org Legal Resources, 'Cyber Bullying Laws', available at: https://www.hg.org/legal-articles/cyber-bullying-laws-40713.

HIPCAR (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean) (2013). *Cybecrime/E-crimes: Model Policy Guidelines and Legislative Texts*, ITU, available at: https://www.itu.int/en/ITU-/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf.

IFEX (2016). 'New Cybercrime Law Is Fundamentally Flawed', available at: https://ifex.org/new-cybercrime-law-is-fundamentally-flawed/.

IFEX (2018). 'Will Trinidad and Tobago's Cybercrime Bill Stifle Media Freedom?', available at: https://ifex.org/will-trinidad-and-tobagos-cybercrime-bill-stifle-media-freedom/.

International Press Institute (2014). 'Grenada Parliament Amends Electronic Defamation Law', available at: https://ipi.media/grenada-parliament-amends-electronic-defamation-law/.

International Press Institute (2019). 'New Cybercrime Bill Threatens Press Freedom in British Virgin Islands', available at: https://ipi.media/new-cybercrime-bill-threatens-press-freedom-inbritsh-virgin-islands/.

International Press Institute (2016). 'St Vincent and Grenadines Adopts Cybercrime Law', *Newsroom*, available at: https://ipi.media/st-vincent-and-grenadines-adopts-cybercrime-law/.

Khoo, C (2021). *Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence*, Women's Legal Education and Action Fund (LEAF), available at: https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf.

KnowProSE.com (2017). 'Public Comment on the Trinidad and Tobago CyberCrime Bill, 2017', available at: https://knowprose.com/2017/06/13/public-comment-on-the-trinidad-and-tobago-cybercrime-bill-2017/.

LatinAmerican Post (2018). 'Alarming Figures of Bullying in Latin America and the Caribbean', available at: https://latinamericanpost.com/24051-the-alarming-figures-of-bullying-in-latin-america-and-the-caribbean.

Law Commission of Ontario (2020). *Defamation Law in the Internet Age*, available at: https://www.lco-cdo.org/en/our-current-projects/defamation-law-in-the-internet-age/.

Law Commission of Ontario (2020). *Executive Summary: Defamation Law in the Internet Age*, available at: https://www.lco-cdo.org/wp-content/uploads/2020/03/Defamation-Executive-Summary-Eng-FINAL.pdf.

Life in Leggings: Caribbean Alliance against Gender-based Violence (2022). Facebook, available at: https://www.facebook.com/officiallifeinleggings/. McGill University (2018). 'Bystanders in Cyberbullying', available at: https://www.mcgill.ca/newsroom/channels/news/bystanders-cyberbullying-288182.

Metri, N (2018). 'Building Awareness of Digital Violence against Barbadian Women', *Internet Society*, available at: https://www.internetsociety.org/blog/2018/07/building-awareness-of-digital-violence-against-barbadian-women/.

MNLSSA Litigator (2015). 'Cyber Law in the Caribbean (Part 2)', available at: https://thenmlssalitigator.wordpress.com/2015/02/26/cyber-law-in-the-caribbean-part-2/.

Mohamed, S (2017). 'Bullying among Students in Princes Town West Secondary', CAPE Caribbean Studies IA, available at: https://www.slideshare.net/Zara_Mohammed/caribbean-studies-ia-71974897. .

Naffi, N (2018). 'Don't Be a Bystander: Five Steps to Fight Cyberbullying', *The Conversation*, Concordia University, available at: https://theconversation.com/dont-be-a-bystander-five-steps-to-fight-cyberbullying-91440.

Organization of American States (1995). *Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women (the Belém do Para Convention)*, available at: https://www.oas.org/juridico/english/treaties/a-61.html.

Organization of American States (2019). 'Violence and Discrimination against Women and Girls: Best Practices and Challenges in Latin America and the Caribbean', Inter-American Commission on Human Rights, available at: http://www.oas.org/en/iachr/reports/pdfs/ViolenceWomenGirls.pdf.

Parliament of Canada (2019). *Taking Action to End Online Hate, Report of the Standing Committee on Justice and Human Rights*, 42nd Parliament, 1st Session (Anthony Housefather, Chair), available at: https://www.ourcommons.ca/Content/Committee/421/JUST/Reports/RP10581008/justrp29/justrp29-e.pdf.

Parliament of Canada (2017). *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 (Marilyn Gladu, Chair), available at: file://localhost/C:/Users/Admin/Documents/Commonwealth/hoc report on violence aginst women 2017.pdf.

Plan International (2020). 'Abuse and Harassment Driving Girls off Facebook, Instagram and Twitter', available at: https://plan-international.org/news/2020–2010–05-abuse-and-harassment-driving-girls-facebook-instagram-and-twitter.

Psychology Today Canada (2022). 'Bystander Effect', available at: https://www.psychologytoday.com/ca/basics/bystander-effect.

Public Safety Canada, Government of Canada (2021). 'Government of Canada Awareness Campaign Addresses Growing Risk of Online Child Sexual Exploitation', available at: https://www.canada.ca/en/public-safety-canada/news/2021/07/government-of-canada-awareness-campaign-addresses-growing-risk-of-online-child-sexual-exploitation.html.

Reporters Without Borders (2017). 'RSF Concerned by Certain Provisions of Trinidad and Tobago's Cybercrime Bill', available at: https://rsf.org/en/news/rsf-concerned-certain-provisions-trinidad-and-tobagos-cybercrime-bill.

Robin, W (2022). 'Bullying, Victims, and Bystanders: From Prevalence to Prevention', University of Pennsylvania, available at: https://www.academia.edu/2896809/Bullies_Victims_and_Bystanders_From_Prevalence_to_Prevention?email_work_card=reading-history.

Royal Canadian Mounted Police (2018). 'Bullying', available at: https://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/pdf/bully-int-eng.pdf.

Royal Canadian Mounted Police (2020). 'Delete Cyberbullying', available at: https://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/video/cyber-video-eng.htm.

Royal Canadian Mounted Police (2020). 'Online safety – Learning Resources', available at: https://www.rcmp-grc.gc.ca/cycp-cpcj/is-si/isres-ressi-eng.htm.

Sheil, R (2016). 'Jamaican Children and the Hidden Dangers of Online Abuse', UNICEF Jamaica, available at: https://blogs.unicef.org/jamaica/unspoken-jamaican-children-online-abuse/.

Shultz, E, R Heilman and KJ Hart (2014). 'Cyber-bullying: An Exploration of Bystander Behavior and Motivation', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 8(4), Article 3.

Smith, T and N Stamatakis (2021). 'Cyber-victimization Trends in Trinidad & Tobago: The Results of an Empirical Research', *International Journal of Cybersecurity Intelligence & Cybercrime*, 4(1), 46–63.

Statistics Canada, Government of Canada (2017). 'Cyberstalking in Canada', available at: https://www150.statcan.gc.ca/n1/pub/11–627-m/11–627-m2017039-eng.htm.

Statistics Canada, Government of Canada (2016). 'Cyberbullying and Cyberstalking among Internet Users Aged 15 to 29 in Canada', in Hango, D, *Insights on Canadian Society*, available at: https://www150.statcan.gc.ca/n1/pub/75–006-x/2016001/article/14693-eng.htm.

Statistics Canada, Government of Canada (2019). 'Gender-based Violence and Unwanted Sexual Behaviour in Canada, 2018: Initial Findings from the Survey of Safety in Public and Private Spaces', in Cotter, A and L Savage, *Juristat*, Catalogue No 85-002-X (Ottawa), available at: https://www150.statcan.gc.ca/n1/pub/85–002-x/2019001/article/00017-eng.htm.

Straatman, A-L (2013). 'Bystander Sexual Violence Education Programs for High School, College and University Students', *Learning Network Brief #9, Learning Network*, Centre for Research and Education on Violence against Women and Children, University of Western Ontario, available at: https://www.vawlearningnetwork.ca/our-work/briefs/index.html.

Trinidad & Tobago Guardian (2015). 'Cyberbullying and Youth', available at: https://www.guardian.co.tt/article-6.2.376401.37bb05bd92.

Trinidad & Tobago Guardian (2015). 'Cyberbullying and Youth, Part Two', available at: https://www.guardian.co.tt/article-6.2.361986.53e547c651.

UNAIDS (2020). 'Caribbean Community Organizations Call for Decisive Action to End Homophobic Abuse and Cyberbullying', available at: https://www.unaids.org/en/resources/presscentre/featurestories/2020/may/20200529_caribbean_homophobia_bullying.

UNESCO (2020). 'International Day against Violence and Bullying at School Including Cyberbullying', available at: https://en.unesco.org/commemorations/dayagainstschoolviolenceandbullying.

UNHCR (2016). 'St. Vincent and the Grenadines Law Would Allow Prison for Defamation Online', Refworld.com, available at: https://www.refworld.org/docid/57b2d22415.html.

Uniform Law Conference of Canada (2020). *Uniform Non-consensual Disclosure of Intimate Images Act: Report of the Working Group and Draft Uniform Act*, available at: https://www.ulcc-chlc.ca/ULCC/media/EN-Annual-Meeting-2020/Report-of-the-Working-Group-and-Draft-Uniform-Act-2020.pdf.

United Nations (2016). *Annual Report of the Special Representative of the Secretary-General on Violence against Children*, UN Human Rights Council, 31st session, available at: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session31/Documents/A_HRC_31_20_E.doc.

United Nations, 'Caribbean Women Count: Ending Violence against Women and Girls Data Hub', UN Women, available at: https://caribbeanwomencount.unwomen.org.

United Nations (2016). Inter-parliamentary Union, 'Sexism, Harassment and Violence Against Women Parliamentarians', United Nations IPU Archive, available at: http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf.

United Nations (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*, by D Šimonović, UNHRC, 38th Sess, UN Doc A/HRC/38/47, available at: https://digitallibrary.un.org/record/1641160?ln=en.

United Nations (2020). "Interpersonal Cybercrime Prevention", UNODC, available at: https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/interpersonal-cybercrime-prevention.html.

United Nations (2020). 'Violence against Children (VAC) in the Eastern Caribbean Area', UNICEF, available at: http://www.iin.oea.org/pdf-iin/materiales-presentaciones/VAC%20in%20the%20Eastern%20Caribbean%20Area.pdf.

United Nations (2021). 'Facts and Figures: Ending Violence against Women', UN Women, available at: https://www.unwomen.org/en/what-we-do/endng-violence/facts-and-figures.

United Nations, "Violence against Women", UN Women, available at: https://www.un.org/womenwatch/daw/vaw/v-overview.htm.

University of Victoria (BC) (2022). "Bystander Intervention", available at: https://www.uvic.ca/services/studentlife/initiatives/bystander-intervention/.

Watt, D and M Fuerst (2021). *Tremeear's Criminal Code, annotated*, Thomson Reuters, available at: https://tinyurl.com/4245hbdj.

West, J (2014). 'Cyber-violence against Women', *Battered Women's Support Services*, available at: http://www.bwss.org/wp-content/uploadeds/2014/05/CyberVAWReportJessicaWest.pdf.

Williams, H and A Campbell (2016). 'A Punch at Cyber Bullying', *Jamaica Observer*, available at: https://www.jamaicaobserver.com/news/a-punch-at-cyber-bullying_78983.

Women's Shelters Canada (2021). 'A Report to Guide the Implementation of a National Action Plan on Violence against Women and Gender-Based Violence', available at: https://www.nationalactionplan.ca/wp-content/uploads/2021/06/NAP-Final-Report.pdf.

Women's Shelters Canada (2017). 'Shelter Voices', available at: https://endvaw.ca/wp-content/uploads/2017/06/shelterVoices_ENG_2017WEB.pdf.

Young, H and E Laidlaw (2020) 'Creating a Revenge Porn Tort for Canada', *Supreme Court Law Review* 147, available at: https://cdn-res.keymedia.com/cms/files/ca/126/0299_637504689539937220.pdf.

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

thecommonwealth.org

The Commonwealth

D19038