# End violence: Women's rights and safety online

# Technology-related violence against women: Recent legislative trends

*Carly Nyst*

*Association for Progressive Communications (APC)*

*May 2014*

Ministry of Foreign Affairs

*This research is part of the APC "End violence: Women's rights and online safety" project funded by the Dutch Ministry of Foreign Affairs (DGIS) and is based on a strong alliance with partners in seven countries: Bosnia and Herzegovina, Colombia, the Democratic Republic of Congo, Kenya, Mexico, Pakistan and the Philippines. For more information visit GenderIT.org and Take Back the Tech!*

**Table of Contents**

## Introduction

This study seeks to explore recent legislative developments aimed at addressing and providing avenues of redress for technology-related violence against women. We explore the objectives, structure and application of four domestic legislative responses to different forms of violence against women, seeking to understand how domestic legislatures are responding to increasing awareness of violence against women online.

The key questions that this report has sought to ask of the legislation include:

1. What is the background to the legislation? Why was it introduced?
2. What was the legislative history of the legislation? What changes were made during the legislative process, and why?
3. What recourse is available through the legislation? Does it criminalise offences related to violence against women online? What provisions are in place to ensure that victims of technology-related violence have access to justice?
4. What are the main critiques of the legislation? What are its primary failings? Has it been successfully applied/invoked to date?

## Report format

This report analyses the following pieces of legislation:

- The South African Protection from Harassment Act 2010
- The Nova Scotia (Canada) Cyber Safety Act 2013
- The California (United States) SB 255 Electronic Communication Devices: Prohibited Distribution of Personal Information
- The New Zealand Harmful Digital Communications Bill 2013.

Analysis of each act is broken down into the following sections

- Introduction
- Background to the legislation
- Legislative history
- Recourse available through the legislation
- Analysis and critique.

The report concludes with a brief synthesis of the common themes running through the legislation, and an analysis of what recent legislative trends suggest about the future development of legislative protections against violence against women online.

# 1. South Africa: Protection from Harassment Act 2010 (the "Cyber Bully Act")

## 1.1. Introduction

The *Protection from Harassment Act 2010* ("the Harassment Act") was adopted by the South African legislature in 2011, and came into force on 27 April 2013. The act provides for a process whereby individuals subject to harassment – either online or off – can apply to the court for a protection order lasting up to five years. The Harassment Act also contains provisions requiring electronic communications service providers to assist the court in identifying individuals responsible for harassment, and creates the offences of contravention of protection orders and failure of an electronic communications service provider to furnish required information.

## 1.2. Background to the legislation

Over the past decade, there have been several prominent incidents of harassment and stalking in South Africa, including the tragic killing of a television journalist, Shadi Rapitso, in 2009.[1] As early as 1999, the South African Law Reform Commission identified stalking as an increasing and complex problem in the country. At that time, the Commission was undertaking a study of the legislative framework related to sexual offences, and it identified stalking as an area that required further examination. The Commission's 1999 *Discussion Paper on Sexual Offences: The Substantive Law*[2] noted that were stalking to be included in legislation specifically aimed at criminalising specific sexual conduct, this would not afford all victims of stalking the protection they required. Moreover, the Commission recognised that although stalking is often associated with domestic violence, it is a problem that is much broader than the domestic sphere. Whereas the *Domestic Violence Act 1998* defines stalking, albeit restrictively, it provides recourse to a person who is stalked only if he or she is in a domestic relationship with the stalker. Including the term harassment in the definition of domestic violence would accommodate some acts amounting to stalking, but further legislative protections were needed.

In November 2006, the Law Reform Commission published a paper dedicated to stalking (Project 130).[3] The paper was a result of a lengthy research and consultation process, which included the development of draft legislation on protection against harassment. The consultation was broad in scope and allowed individuals and civil society groups to provide input; around 30 submissions were received by the Commission. A draft version of the report was also circulated and open for comments. In the report the Commission made 27 recommendations, the most pertinent of which relate to:

- The inadequacy of the (then) existing civil law framework to provide recourse to victims of stalking who are not in a domestic relationship.
- The need for legislation (i.e. the Protection from Harassment Bill) to be enacted to specifically cater for a civil remedy for stalking and thereby provide legislative recourse to victims of stalking as understood in the broader sense.
- The inclusion of direct or indirect conduct in the definition of harassment.
- The importance of providing an avenue by which application for redress can be made on behalf of those victims of stalking who are unable to do so in their own name.

[1] Capazorio, B. (2013, February 13). Stalking victims vulnerable. *IOL News*. www.iol.co.za/news/south-africa/stalker-victims-vulnerable-1.1025429#.UzXNglF_s6I
[2] South African Law Reform Commission. (1999). *Discussion Paper on Sexual Offences: The Substantive Law (Project 107)*. Discussion Paper 85.
[3] South African Law Reform Commission. (2006). *Report on Stalking (Project 130)*. www.justice.gov.za/salrc/reports/r_pr130_stalking.pdf

- The inclusion in the legislation of a judicial discretion to order the seizure of a firearm or a dangerous weapon on granting an interim or final protection order.
-

Importantly, the Commission recommended against the enactment of an explicit crime of stalking in South Africa. It noted that stalking behaviour is addressed by way of a number of existing offences, such as assault, crimen injuria, trespassing or malicious damage to property. The Commission was of the view that an improved understanding and application of the existing law would acknowledge the rights of certain victims of stalking to redress in terms of the criminal law and provide immediate intervention, provided relevant government departments developed practical mechanisms to enable individuals to effectively use the existing avenues for redress.

While harassment by electronic means was included in the definition of harassment in the proposed Protection from Harassment Bill drafted by the Commission, there was no provision in the original draft for any role of electronic communications service providers in supplying information or facilitating the identification of the respondent to an application for a protection order.

## 1.3. Legislative history

The Protection from Harassment Bill drafted by the Commission was introduced into the National Assembly on 31 January 2010. After the first reading of the bill, the Portfolio Committee on Justice and Constitutional Development considered the bill and subsequently introduced the provisions requiring the cooperation of electronic communications service providers.[4] These amendments reflected concerns expressed by, among others, WomensNet, who highlighted the need to recognise online harassment and make provision for redress by individuals who do not know the identity of their harasser.[5]

The Committee also raised the question of whether the bill should create an offence of making false applications for protection orders, but decided against including such a provision. Nevertheless, when reporting back on its findings at the second reading of the bill on 16 August 2011, the Committee called upon the Ministry to give serious consideration to this matter.[6]

A further change made between the first and second readings of the bill was the amendment of the considerations that must be taken into account when considering whether conduct is unreasonable, including whether the conduct is being engaged in for the purpose of detecting or preventing an offence, in order to reveal a threat to public safety or the environment, to reveal an undue advantage in a competitive bidding process, or to comply with a legal duty. The driving factor behind these amendments was the concern expressed in public hearings by the media,[7] particularly investigative journalists, that they would be prevented from undertaking activities central to their profession if the powers under the bill were misapplied.[8]

With the exception of the critiques levelled by the media, the bill generally received support from across

[4] www.pmg.org.za/hansard/20110816-second-reading-debate-military-veterans-bill-b-1b-%E2%80%93-2011-protection-
[5] Shukumisa. (2010). Public hearings on Protection from Harassment Bill take place today. *Shukumisa*. www.shukumisa.org.za/index.php/2010/10/public-hearings-on-protection-from-harassment-bill-take-place-today
[6] www.pmg.org.za/hansard/20110816-second-reading-debate-military-veterans-bill-b-1b-%E2%80%93-2011-protection-
[7] SAPA. (2011, August 17). Protection from harassment bill approved. *News24*. www.news24.com/SouthAfrica/Politics/Protection-from-harassment-bill-approved-20110816
[8] DefenceWeb. (2011, June 20). Media safeguard inserted in Protection from Harassment Bill. *DefenceWeb*. www.defenceweb.co.za/index.php?option=com_content&view=article&id=16372:media-safeguard-inserted-in-protection-from-harassment-bill-&catid=54:Governance&Itemid=118

the political spectrum, and there were no arguments against its adoption. Ultimately, the bill was adopted by the National Assembly on 8 November 2011,[9] assented to by the president on 2 December 2011,[10] and gazetted on 5 December 2011.[11]

### 1.4. Recourse available through the Act

The primary intention of the Harassment Act[12] is to set up a system whereby an individual can apply to the court for a protection order against another person to stop that person harassing them. The system is free to the complainant and does not require them to have legal representation [s2(2)]. Applications can be brought by someone acting on behalf of a victim of harassment [s2(3)], and can also be brought by children without parental permission [s2(4)].

The act sets up a number of stages for the issuing of a protection order:

1. An individual (the complainant) can apply for a protection order if they are *subject to harassment*, which includes conduct that the harasser (the respondent) knows or ought to know (s1):
    a. Causes harm or inspires the reasonable belief that harm may be caused to the complainant or a related person by unreasonably:
        i. following, watching, pursuing or accosting the complainant or a related person, or loitering outside of or near the building or place where the complainant or related person resides, works, carries on business, studies or happens to be.
        ii. engaging in verbal, electronic or any other communication aimed at the complainant or a related person, by any means, whether or not conversation ensues.
        iii. sending, delivering or causing the delivery of letters, telegrams, packages, facsimiles, electronic mail or other objects to the complainant or a related person or leaving them where they will be found by, given to, or brought to the attention of, the complainant or a related person.
    b. Amounts to sexual harassment of the complainant or a related person.

2. The complainant *makes an application* for a protection order to the court, with an affidavit in support of their application. If the court is satisfied that there is prima facie evidence that the respondent is engaging or has engaged in harassment; that harm is being suffered or may be suffered by the complainant or a related person if a protection order is not issued immediately; and the protection accorded by a protection order will not be achieved if the respondent has prior notice of the application, it must issue an interim protection order against the respondent [s3(2)].

3. After the issuing of an interim protection order, *the respondent is served with notice of the order*, a copy of the application, and a request to show cause on the return date specified (not less than 10 days after service) why the interim protection order should not be made final [s3(3)].

4. At the same time as issuing the interim protection order (and again when issuing a protection order), the court must make an order authorising the *issue of a warrant for arrest*, and immediately suspending the execution of the warrant subject to the compliance with the order [s11(1)]. At any time while an interim protection order (or protection order) is in force, a complainant can take a copy of the warrant, with an affidavit, to any member of the South African Police Service and allege the commission of an offence by way of contravention of the order

[9] SAPA. (2011, August 17). Op. cit.
[10] SabinetLaw. (2011, December 7). President Gives Nod to Protection From Harassment Act. *SabinetLaw*. www.sabinetlaw.co.za/justice-and-constitution/articles/president-gives-nod-protection-harassment-act
[11] www.pmg.org.za/bill?year=2010
[12] www.acts.co.za/protection-from-harassment-act-2010/

[s11(4)]. The act makes any contravention of an order a criminal offence punishable by a fine or imprisonment not exceeding five years [s18(1)].

5. If the *identity of the respondent is not known*, the court may take the following steps to assist the complainant:
    a. Order an *electronic communications service provider* to furnish the court with information about the identity of the respondent, and any information about communications sent by the respondent as are available (s4).
    b. Order the *police service* to take necessary measures to obtain information about the identity of the respondent (s5).

6. The court can hold proceedings in private and *prevent the publication of information* about the proceedings (s8). It can also *subpoena any person to appear as a witness* or to provide any document or thing relevant to the proceedings (s7).

7. If the *respondent does not reply* to the notice of the interim protection order, the court must issue a protection order, which remains in force for up to five years. If the respondent does reply and *opposes the issuing of a protection order*, the court must hear further evidence. Prior to issuing a protection order, it must be satisfied, on the balance of probabilities, that the respondent has engaged or is engaging in harassment of the complainant (s9).

8. Protection orders can include the following provisions (s10):
    a. Prohibiting the respondent from engaging in harassment themselves or enlisting another's help to do so.
    b. Committing any other act specified in the order.
    c. Complying with any other provision which the court deems reasonably necessary.
    d. Requiring the police service to seize any weapon in the respondent's possession.

9. In addition to establishing the offence of contravention of a protection order, the act also *establishes offences* with respect to:
    a. Revealing the identities of the parties or publishing information in contravention of the court's orders [s 18(2)]
    b. Electronic communications service providers failing to furnish information or making a false statement [s18(4)].

## 1.5. Analysis and critique

***Creation of offences***

The act provides a vital mechanism for redress for victims of harassment outside of domestic relationships. Importantly, it has an expansive definition of conduct that constitutes harassment, including that which is effected by electronic means, and seeks to address the anonymity afforded by the internet and ICTs by creating obligations upon service providers to facilitate the identification of those accused of harassment.

However, the Harassment Act does not provide for harassment or stalking to be considered as a crime. This option was considered and discarded by the drafters, who considered such crimes already sufficiently covered by existing common law criminal actions. This fact is reflected in the act, which requires the clerk of the court to inform any unrepresented complainant of their right to lodge a criminal complaint against

the respondent of crimen injuria, assault, trespass, extortion or any other offence which has a bearing on the persona or property of the complainant [s2(2)(b)].

This may be seen by some as a deficiency of the act. Nevertheless, cases of harassment have been successfully prosecuted in South Africa under the above-named criminal actions, and there is no suggestion that South African law is insufficient in this respect. Therefore, this act, rather than focusing on criminalising the perpetrators, directs itself towards providing actual relief from harassment for the complainant. Such focus may be seen as a response to the particular social affordances of ICTs.

The act does create offences around failure to comply with a protection order issued under the act, and failure of an electronic communications service provider to provide information requested under the act. These are important accountability mechanisms. In the case of the latter, the act even stipulates that an individual employee of an electronic communications service provider can be liable for a fine or imprisonment if they fail to comply with an order. Such provisions provide a strong statement about the force and importance of the legislation.

***Definition of harassment***

The definition of harassment contained in the act is, on its face, broad enough to encompass the wide range of conduct that may constitute harassment. For example, the inclusion of actions such as the sending of electronic mail, and engaging in electronic communication whether or not conversation ensues, would encompass a considerable range of frequent actions taken by online harassers, including the sending or publication of photographs or images of victims. However, the application of the legislation will depend on the courts' interpretation of the alleged offence.

Time will also tell how the courts interpret the other terms within the law that qualify harassment under the act, particularly the concepts of "inspires the reasonable belief" and "unreasonably" in the context of the definition of harassment. An expansive interpretation of these terms will benefit victims of harassment, but if a strict interpretation is taken it may limit the effectiveness of the act.

***Effectiveness and implementation***

There have been no published applications under the Harassment Act to date, so it is difficult to yet assess how effectively it is being implemented. While the act has been positively received, some commentators have noted the need for greater education and stronger efforts at implementation. During the consultations on the act, the Women's Legal Centre drew analogies with the procedures available under the Domestic Violence Act, where despite the existence of the legislation, the police have treated numerous women who file complaints of domestic violence with complete disregard and/or a lack of professionalism.[13] Their critique highlights the need for initiatives to educate both the public and the police force about the problems associated with harassment and the need to take decisive action to address it.

[13] Sutherns, T. (2011, March 28). The Protection from Harassment Bill. *Victim Empowerment Law South Africa*. victimempowermentlaw.org.za/2011/03/28/the-protection-from-harassment-bill

# 2. Nova Scotia, Canada: Cyber Safety Act 2013 – An Act to Address and Prevent Cyberbullying (the "Cyber Bullying Act")

## 2.1. Introduction

The *Cyber Safety Act 2013*[14] was adopted by the Nova Scotia General Assembly in May 2013 and came into force on 6 August 2013. The act provides for a process whereby individuals subject to cyber bullying (or, in the case of minors, their parents) can apply to a justice for a protection order against an individual. The Cyber Safety Act contains provisions requiring electronic communications service providers to assist the court in identifying individuals responsible for cyber bullying. The act also creates the tort of cyber bullying, enabling individuals to sue another for damages arising out of cyber bullying.

## 2.2. Background to the legislation

The legislation came about as a direct result of the death of 17-year-old Nova Scotia student Rehtaeh Parsons, who took her own life after having been subject to months of harassment and humiliation stemming from the dissemination online of a photo of her being allegedly sexually assaulted. She died on 7 April 2013; three weeks later, the Cyber Safety Bill was introduced into the Nova Scotia provincial parliament. Rehtaeh's parents were leading advocates for the legislation.[15]

## 2.3. Legislative history

The Cyber Safety Bill (Bill 61) was introduced in the General Assembly on 25 April 2013 by Representative Marilyn More.[16] The second reading of the bill took place the following day, at which time it was adjourned to the Committee on Law Amendments for scrutiny. The Committee returned the bill on 7 May 2013 without amendments, at which time it was adjourned for a third reading on 10 May 2013.

During the third reading on 10 May 2013, Representative More noted the consultative process that had taken place during the preparation of the bill:

> We've been meeting with community and women's groups, youth, health and educational professionals, and others to identify gaps in services for those affected by cyberbullying and sexual assault. We've made an additional $900,000 available for programs across the province to support victims of sexual violence, and we are reviewing the actions of all agencies involved and coordinating a provincial education campaign to ensure Nova Scotians know where to get help if they need it.[17]

She also noted that amendments suggested by the opposition were incorporated into the bill.[18] It is unclear what those amendments were, although it appears they were not major. The act was adopted after the third reading on 10 May 2013. It is unclear from the Hansard record how many parliamentarians voted for or against the act.

[14] www.canlii.org/en/ns/laws/stat/sns-2013-c-2/latest/part-1/sns-2013-c-2-part-1.pdf
[15] Davison, J. (2013, August 12). Can cyberbullying laws really work? *CBC*. www.cbc.ca/news/canada/can-cyberbullying-laws-really-work-1.1367611
[16] nslegislature.ca/legc/PDFs/annual%20statutes/2013%20Spring/c002.pdf
[17] nslegislature.ca/index.php/proceedings/hansard/C90/house_13may10, p. 2515.
[18] Ibid.

## 2.4. Recourse available through the act

The Cyber Safety Act has a number of different elements that provide redress to victims of online bullying and harassment. Throughout, "cyberbullying" is defined to mean [s3(1)]:

> *[A]ny electronic communication through the use of technology* including, without limiting the generality of the foregoing, computers, other electronic devices, social networks, text messaging, instant messaging, websites and electronic mail, *typically repeated or with continuing effect*, that is *intended or ought reasonably be expected* to cause *fear, intimidation, humiliation, distress or other damage or harm* to another person's *health, emotional well-being, self-esteem or reputation*, and includes assisting or encouraging such communication in any way.

The act stipulates that if a minor engages in an activity that is cyber bullying, and their parent knew of the activity, and knew or ought reasonably have expected the activity to cause the requisite fear or harm, and failed to take any steps to prevent the activity, the parent is deemed to have engaged in cyber bullying [s3(2)].

***Protection orders***

The act establishes a protection order scheme to enable a victim of cyber bullying (or their parents) to obtain an order preventing and punishing cyber bullying, or mandating a person responsible for cyber bullying to take certain steps. An application for a protection order can be submitted on behalf of a minor by their parent, a designated person, or a police officer [s5(1)]. An application can be made [s5(4)] and evidence given [s6(2)] by telephone or other means of telecommunication. There is to be no publication of the name or information likely to identify any minor involved in a proceeding relating to an application for a protection order (s16).

The act sets up a number of stages for the issuing of a protection order:

1. A subject of cyber bullying (the subject) can *apply to a justice for a protection order* without notice to the respondent [s5(1)].

2. The application must *name as a respondent any person associated with an electronic device*, Internet Protocol address, website, username or account, electronic mail address or other unique identifier, identified as being used for cyber bullying, or a parent of the person if the person is a minor [s5(2)].

3. *If the name of the respondent is unknown*, the application should stipulate the IP address, username or other identifier [s5(3)]. The justice can issue an *order to any person having custody or control of information* (including ownership of devices or accounts) pertaining to the identification of the respondent (s7).

4. If the justice is satisfied that, *on a balance of probabilities*, the respondent engaged in cyber bullying and there are reasonable grounds to believe they will continue to do so, the justice may issue a protection order (s8), including any of the following provisions [s9(1)]:
    a. Prohibiting the respondent from engaging in cyber bullying, directly or indirectly communicating with or about or contacting the subject.
    b. Prohibiting or restricting the respondent from using a specified or any means of electronic communication.
    c. Confiscating any electronic device capable of connecting to an IP address associated with

the respondent.

d. Discontinuing the respondent's internet access.
e. Any other order for up to one year [s9(2)].

5. The protection order is *served on the respondent*, at which time they become bound by it [s11(2)], and is also served on the subject or their parents [s11(4)-(5)].

6. Within a period set down by the regulations, the *court shall review the justice's order* and, if satisfied that there was sufficient evidence to support the justice's making of the order, shall confirm or vary the order [s12(1)-(2)].

7. If the court *is not satisfied there is sufficient evidence*, it shall direct a hearing of the matter, after which time the court may confirm, terminate or vary the protection order [s12(3)-(7)].

8. The court can *remove, vary, amend or revoke the protection order* at any time after the order is confirmed [s13)].

9. The act *creates an offence* of contravention of a protection order (s19), carrying with it a fine of not more than CAD 5,000 or six months imprisonment, or both. It also creates an offence of publication of information about the identity of a minor and of contravention of an order prohibiting the publication of identity information [s18)].

***Tortious liability***

The Cyber Safety Act also creates the tort of cyber bullying (s21), in an action for which a court may award damages, issue an injunction, or make any other order [s22(1)]. This means that, separately from an application for a protection order to prevent future cyber bullying, a victim of cyber bullying or their parents can make a claim against the perpetrator of cyber bullying for past cyber bullying and seek an award of damages.

The legislation stipulates that where the defendant in a tortious action for cyber bullying is a minor, a parent of the defendant is jointly and severally liable for any damages unless the parent satisfies the court that they were exercising reasonable supervision over the defendant and made reasonable efforts to prevent or discourage the defendant from engaging in cyber bullying [s22(3)].

***Cyber bullying prevention order***

The Cyber Safety Act also amends the *Safe Communities and Neighbourhoods Act 2006*[19] ("Safe Communities Act") to establish a CyberSCAN unit[20] tasked with investigating complaints related to cyber bullying, issuing warning letters, requesting an internet service provider to discontinue service, or applying to the court for an order requiring the production of information about the identity of an individual accused of cyber bullying (s26B of the Safe Communities Act). In response to an application by a director of public safety, the court may issue an order requiring information to identify who may have used an IP address, website, account or username, or particular device; and to produce cell phone records, text message records, internet browsing history records and any other records that would assist in investigating the complaint [s26C(2)]. The CyberSCAN unit has a website,[21] although it does not publish information about

[19] nslegislature.ca/legc/statutes/safer%20communities%20and%20neighbourhoods.pdf
[20] CBC News. (2013, April 25). N.S. cyberbullying investigative unit a 1st in Canada. *CBC*. www.cbc.ca/news/canada/nova-scotia/n-s-cyberbullying-investigative-unit-a-1st-in-canada-1.1359308
[21] cyberscan.novascotia.ca

the cases that it has dealt with.

The director of public safety can also apply to the court for a cyber bullying prevention order (s26D), upon which the court can take similar steps as those prescribed under the protection order procedures (s26G).

## 2.5. Analysis and critique

***Implications for free expression***

The introduction of the Cyber Safety Act was not uncontroversial. The act has faced criticism from free expression advocates who say that the definition of "cyberbullying" contained in the act is too broad, and the scope of powers afforded to a justice or court issuing a protection order too wide.[22] The breadth of the powers available to the court is considerable and could have serious implications for the individual subject to them. Restricting access to the internet and to a particular technological device are punitive measures that have the simultaneous effect of limiting access to information and preventing the free expression of ideas, access to education, as well as the freedom to associate. While they are appropriate measures in the correct circumstances, given that the legislation only requires that the complainant meet a relatively low threshold of proof – a justice must be satisfied on the balance of probabilities that a behaviour has occurred – this could enable abuse of the system, imperilling the rights of the respondent.[23]

***Parental responsibility***

The act takes a strict approach to parental liability with respect to activities undertaken by their children. While this may be an important mechanism for improving parental responsibility, it may also penalise single-parent families, immigrants and those who have language difficulties. The liability technically lies on parents who were already aware or made aware of their children's behaviour and took no steps to stop it. However, parents with long working hours may not have the time to monitor their children's online behaviours; those who are not literate in social media and digital technologies themselves may not be aware of how to stop or prevent such actions by their children.[24]

***Effectiveness and implementation***

The Cyber Safety Act was invoked for the first time in February 2014, when the director of public safety applied for a cyber bullying prevention order under s26D of the act. The case pertained to allegations by the chief of the Pictou Landing First Nation who alleged that Christopher Prosper was posting negative and threatening comments about her and her family on several Facebook sites. According to an affidavit from Dana Bowden, an officer with Nova Scotia's CyberSCAN unit, Prosper called Paul a "crook, backstabbing bitch, two-faced to our elders. Your fake smile needs a punch in the face."[25]

After the hearing on 11 February 2014, a judge granted a prevention order compelling Prosper to cease all future cyber bullying against Paul and remove any current statements from the internet. The court also ordered him to pay Paul CAD 750 in court costs. The order stands for one year. The CyberSCAN unit can

[22] Cushing, T. (2013, August 14). Nova Scotia's New Cyberbullying Law Will 'Make Bullies Of Us All'. *Techdirt*. www.techdirt.com/articles/20130812/09495224145/nova-scotias-new-cyberbullying-law-will-make-bullies-us-all.shtml
[23] Globe and Mail. (2014, February 17). Nova Scotia's cyberbullying law goes too far. *The Globe and Mail*. www.theglobeandmail.com/globe-debate/editorials/nova-scotias-cyber-bullying-law-goes-too-far/article16907312
[24] Davison, J. (2013, August 12). Op. cit.
[25] Canadian Press. (2014, February 3). Cyberbullying law faces first courtroom test in Nova Scotia. *CBC*. www.cbc.ca/news/canada/nova-scotia/cyberbullying-law-faces-first-courtroom-test-in-nova-scotia-1.2521807

then apply for an extension if it feels the cyber bullying is continuing.[26]

The CyberSCAN unit has received 93 complaints since it was established in September 2013. Over half of the complaints are still active, while the remainder were either informally resolved, handed over to police or did not require further action.[27]

In addition, critics have argued that the law, while an important symbolic move, is insufficient to address systemic bullying and cyber bullying issues amongst Nova Scotian youth. The lack of awareness among the youth of the problems with cyber bullying, as well as the avenues of redress available, is borne out by evidence which shows that the bulk of complaints brought before the CyberSCAN unit have been made by adults.

Critics have noted that the legislation will only be effective as long as other forms of prevention, intervention and education are in place.[28] In the words of Marvin Bernstein, the chief policy adviser at UNICEF Canada:

> The more important and more impactful approaches really relate to prevention and education. And before we vilify the cyberbullies, I think we need to recognize that a good number of the cyberbullies are really children or young people themselves, and that when they carry out this kind of behaviour in many instances they don't understand the impact of what they are doing.[29]

[26] CBC News. (2014, February 11). Judge orders end to Facebook cyberbullying under new law. *CBC*. www.cbc.ca/news/canada/nova-scotia/judge-orders-end-to-facebook-cyberbullying-under-new-law-1.2531764
[27] CBC News. (2013, 25 de abril). Op. cit.
[28] Davison, J. (2013, 12 de agosto). Op. cit.
[29] Ibid.

# 3. California, USA: SB 255 Electronic Communication Devices: Prohibited Distribution of Personal Information law

## 3.1. Introduction

SB 255 Electronic Communication Devices: Prohibited Distribution of Personal Information was signed into effect by California Governor Jerry Brown on 1 October 2013, having passed the state legislature after months of amendments. The law amends the Penal Code to create a new misdemeanour of disorderly conduct by way of distribution of intimate photographs with the intent to cause serious emotional distress. The law is narrowly worded and focused on instances in which the person who takes or makes the intimate image distributes it with the intent to cause, and the effect of causing, serious emotional distress to the victim. The law has been controversial and was staunchly opposed by free expression advocates throughout its drafting.

## 3.2. Background to the legislation

The Prohibited Distribution of Personal Information law grew out of a spate of incidents[30] in which individuals – usually women – had nude or sexually explicit photographs of themselves published online by a previous partner. A number of these incidents became public and spurred legislatures across the United States to consider adopting legislation specifically addressing this form of online harassment or abuse, particularly after a number of women came forward to complain that their experiences had not been appropriately dealt with under existing criminal or civil laws.[31] The Cyber Civil Rights Initiative[32] – a group founded by victims of "revenge porn" and other forms of online harassment – has played a key role in advocating for the adoption of cyber harassment and revenge porn laws across the US, through their End Revenge Porn campaign.[33]

While there was already a movement towards the enactment of revenge porn laws, the California legislation seems to have been particularly spurred by the death of Audrie Pott, a 15-year-old Californian student who committed suicide after photos of her sexual assault were published online.[34] The California state senator who introduced the bill, Republican Anthony Cannella, also consulted with anti-revenge porn activists and parents of those who had been victims of the distribution of private photos and personal information online.

## 3.3. Legislative history

The bill, entitled SB 255 Electronic Communication Devices: Prohibited Distribution of Personal Information, was introduced in the California Senate by Republican State Senator Anthony Cannella on 7 May 2013.[35] The bill proposed to make it a misdemeanour for:

> [A]ny person who, with the intent to cause substantial emotional distress or humiliation to an-

[30] Brill, S. (2014, February 25). The Growing Trend of 'Revenge Porn' and the Criminal Laws That May Follow. *The Huffington Post*. www.huffingtonpost.com/steven-brill/the-growing-trend-of-revenge-porn_b_4849990.html
[31] Chiarini, A. (2013, November 19). I was a victim of revenge porn. I don't want anyone else to face this. *The Guardian*. www.theguardian.com/commentisfree/2013/nov/19/revenge-porn-victim-maryland-law-change
[32] www.cybercivilrights.org
[33] www.endrevengeporn.org
[34] Francis, M. (2013, April 12). Calif. Teens Arrested on Sexual Assault Charges After Girl's Suicide. *NBC*. www.nbclosangeles.com/news/national-international/Teens-Arrested-on-Sexual-Assault-Charges-Following-Saratoga-Suicide-202683071.html
[35] www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0251-0300/sb_255_bill_20130507_amended_sen_v98.html

other person, by means of an electronic communication device, and without consent of the other person, electronically distributes, publishes, emails, hyperlinks, or makes available for down-loading nude images of the other person along with personal identifying information of the other person.

The bill proposed to amend the Penal Code to make the following activities misdemeanours:

- The distribution by electronic communication device of specified identifying information (including a digital image of another person, or an electronic message of a harassing nature about another person) with the intent to place another person in reasonable fear for their safety or that of their immediate family.
- The distribution by electronic communications device of nude images of another person along with personal identifying information.

However, after its introduction the bill was debated in numerous committees, in the Legislative Assembly, and then again in the Senate, over a period of five months. The bill went through a number of iterations[36] and was subject to multiple amendments which resulted in a considerable weakening of the provisions therein.[37] The original text of the bill was opposed by First Amendment advocates such as the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation, which argued that the bill could result in criminalisation of speech, particularly as it was designed to criminalise what they labelled "victimless instances", where no individual was able to demonstrate that they experienced harm as a result of the action.[38] During the third reading of the bill, on 17 June 2013, the ACLU argued:

> The posting of otherwise lawful speech or images even if offensive or emotionally distressing is constitutionally protected. The speech must constitute a true threat or violate another otherwise lawful criminal law, such as stalking or harassment statute, in order to be made illegal. The provisions of this bill do not meet that standard. (See e.g., United States v. Cassidy, (D.Md.2011) 814 F. Supp. 2d 574), wherein the state sought to prosecute a defendant who had tweeted and blogged offensively about a religious figure in Maryland because the defendant intended to harass and cause substantial emotional distress and succeeded in causing such distress. The court held that such conduct could not present a crime. We urge the author to reconsider this proposal.[39]

The ACLU advocated for an amendment to the bill to include, as a condition of the crime, that the parties must have established an agreement or understanding that the image should remain private, and the image was subsequently distributed in violation of that agreement.

On 1 October 2013 the bill was signed into law by Governor Jerry Brown, making California the second state, following New Jersey, to enact a revenge porn law.[40] The resulting legislation[41] amended the Penal Code to include the following provision:

> (4) (A) Any person who photographs or records by any means the image of the intimate body part or parts of another identifiable person, under circumstances where the parties agree or understand

[36] leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml

[37] Gershman, J. (2013, August 22). California Lawmakers Retool Cyber-Revenge Bill. *The Wall Street Journal*. blogs.wsj.com/law/2013/08/22/california-lawmakers-retool-cyber-revenge-bill

[38] Sankin, A. (2013, June 5). Revenge Porn: California Legislators Go After Troubling New Trend. *The Huffington Post*. www.huffingtonpost.com/2013/06/05/revenge-porn-california_n_3391638.html

[39] www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0251-0300/sb_255_cfa_20130703_114233_sen_floor.html

[40] Roy, J. (2013, October 3). California's New Anti-Revenge Porn Bill Won't Protect Most Victims. *Time*. nation.time.com/2013/10/03/californias-new-anti-revenge-porn-bill-wont-protect-most-victims

[41] leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB255#

that the image shall remain private, and the person subsequently distributes the image taken, with the intent to cause serious emotional distress, and the depicted person suffers serious emotional distress.

(B) As used in this paragraph, intimate body part means any portion of the genitals, and in the case of a female, also includes any portion of the breasts below the top of the areola, that is either uncovered or visible through less than fully opaque clothing.

### 3.4. Recourse available through the act

The final law amended the Penal Code to provide for a new crime of disorderly conduct by way of distribution of intimate photographs with the intent to cause serious emotional distress. The crime is punishable by a period of imprisonment not exceeding six months and a fine of USD 1,000 for a first offence, and a period of imprisonment not exceeding one year and a fine of USD 2,000 for a subsequent offence or if the victim is a minor.

The law is narrowly crafted, with the following restrictions:

- The person who distributes the image must have been the same person who created/recorded the image.
- The parties must have agreed or understood that the image would remain private.
- An intimate body part means any portion of the genitals, and in the case of a female, also includes any portion of the breasts below the top of the areola, that is either uncovered or visible through less than fully opaque clothing.
- The offence requires an intent on the part of the distributor of causing serious emotional distress, and requires a victim to suffer serious emotional distress as a result.

The law thus fails to capture or excludes the following forms of online harassment/revenge porn:

- If the image distributed was originally made or taken by the victim themselves (i.e. a "selfie").
- When a third person redistributes an image that they didn't take themselves – including intermediaries such as operators of websites encouraging users to post revenge porn.
- If an image is illicitly taken from a person's computer by a hacker and then redistributed.
- Where there is a dispute of the confidentiality of the image; for example, if the victim never consented to the image being recorded, or where the victim and the defendant disagree about their expectations for the recording.
- Where there is insufficient evidence that the defendant intended to cause the victim severe emotional distress.[42]

There are other means of redress available under Californian law that might be applicable in some of the cases that are excluded by the revenge porn law, anti-hacking laws, copyright laws, and privacy laws. Anti-stalking and anti-harassment laws also can apply to instances where videos of sexual acts are taken without consent and distributed, specifically with intent to hurt the victim.[43] However, where an image was consensually made it was not previously captured by Californian state criminal laws, and victims only had recourse in the form of a civil suit. From that perspective, the changes to the Penal Code have provided an important – if extremely narrow – form of recourse for revenge porn victims.

[42] Goldman, E. (2013, October 8). California's New Law Shows It's Not Easy To Regulate Revenge Porn. *Forbes*. www.forbes.com/sites/ericgoldman/2013/10/08/californias-new-law-shows-its-not-easy-to-regulate-revenge-porn
[43] Ibid.

## 3.5. Analysis and critique

***Narrow scope***

Natalie Webb, director of communications at the Cyber Civil Rights Initiative, says of the legislation: "It's a good first step. But it doesn't really offer meaningful coverage to most victims who have reached out to us. I've answered the e-mails of victims who reach out to us and the truth is, this won't protect many of them."[44]

The narrow scope of the law is the focus of the large majority of criticism that has been levelled at the revenge porn provision. The fact that the legislation excludes "selfies" is of the greatest concern, particularly given that the Cyber Civil Rights Initiative estimates that 80% of revenge porn images were recorded by the victims themselves.

Holly Jacobs, the founder of the Cyber Civil Rights Initiative and herself a revenge porn victim, believes much of the pushback that came from California legislators was rooted in "victim blaming". "If you want my honest opinion as to why this law is so weak, I believe it was unfortunately due to victim-blaming on the part of other legislators," Jacobs said in an email. One bill drafter, Jacobs said, told her that people who take intimate self-shots are "stupid".[45]

However, other anti-revenge porn activists have emphasised that it was important to pass a bill which can be expanded later. "The future plan is to make an amendment so that self-shots are covered," remarked Charlotte Laws, an anti-revenge porn activist. "But I do feel like California has wiped away some tears and pain with the passage of this law." Laws's daughter, Kayla, was the victim of revenge porn when a hacker allegedly stole intimate photos she had taken of herself from her computer.

***Free expression implications***

While numerous civil liberties organisations levelled complaints about the free speech implications of earlier drafts of the law, the final legislation is so narrow in scope as to no longer raise serious considerations from this perspective.

***Implementation***

There have been no prominent prosecutions under the new provision of the Penal Code to date. In December 2013 the California attorney general charged the operator of a revenge porn website but did so relying upon identity theft or extortion statutes, rather than the new law.[46]

[44] Roy, J. (2013, October 3). Op. cit.
[45] Ibid.
[46] Schwartzbach, M. (2013, December 11). The Revenge Porn Prosecution That Wasn't. *Uncuffed*. uncuffedcrime.blogspot.co.uk/2013/12/the-revenge-porn-prosecution-that-wasnt.html

# 4. New Zealand: Harmful Digital Communications Bill 2013

## 4.1. Introduction

The *Harmful Digital Communications Bill* ("the HDCB") was introduced in the New Zealand parliament on 5 November 2013, in follow-up to a study conducted by the Law Commission. The bill provides that its purpose is to mitigate harm caused to individuals by digital communications (a digital communication includes any text message, writing, photograph, picture or recording) and to provide victims of harmful digital communications with a quick and efficient means of redress. The bill creates a new civil enforcement regime for harmful digital communications and creates new criminal offences to deal with the most serious harmful digital communications.

## 4.2. Background to the legislation

The Harmful Digital Communications Bill was introduced in the aftermath of the October 2013 "Roastbusters" sex scandal in New Zealand, in which a group of Auckland men allegedly lured young girls into group sex and then posted the video of the incidents online.[47] However, Justice Minister Judith Collins had mooted the introduction of the bill in April 2013, based on recommendations from the Law Commission. The Law Commission originally prepared a briefing for the justice minister in May 2012, which appended a draft bill. The briefing came at the request of the minister, who asked the Law Commission to fast-track this aspect of the Commission's broader review of media regulation in response to growing community concern about the harm resulting from the misuse of new communication technologies.[48]

## 4.3. Legislative history

The Harmful Digital Communications Bill was introduced in parliament by Justice Minister Judith Collins on 5 November 2013. The first reading of the bill was on 3 December 2013, after which time it was referred to the Justice and Electoral Committee for consideration. The Committee received submissions on the bill until 21 February 2014, and will submit its report in response to its consultation by 3 June 2014.[49]

At the first reading of the bill, Acting Minister of Justice Chester Borrows remarked:

> The Harmful Digital Communications Bill provides for quick, effective, and proportionate responses to the harm caused by digital communications. The bill sets out 10 communication principles to guide the work of the approved agency for the courts. For example, "a digital communication should not be threatening, intimidating, or menacing." Let me be clear that this bill is not aimed at censoring debates and robust exchanges of ideas, or suppressing speech online. Freedom of speech is something this Government and all New Zealanders value. However, free speech is not an absolute right. It must be balanced with other rights and freedoms. The bill strikes the appropriate balance between freedom of speech and protecting people from being bullied or victimised. It also requires the agency and the courts to act consistently with the New Zealand Bill of Rights Act to avoid any doubt about the importance of our fundamental rights.[50]

[47] Vance, A., and O'Callaghan, J. (2013, November 5). 'Time's up' for cyber tormentors. *The Press*. www.stuff.co.nz/the-press/news/schools/9363305/Times-up-for-cyber-tormentors

[48] Law Commission. (2013, November 5). Law Commission welcomes Harmful Digital Communications Bill. *Law Commission*. www.lawcom.govt.nz/news/2013/11/law-commission-welcomes-harmful-digital-communications-bill

[49] www.parliament.nz/en-nz/pb/legislation/bills/00DBHOH_BILL12843_1/harmful-digital-communications-bill

[50] www.parliament.nz/en-nz/pb/debates/debates/50HansD_20131114_00000024/harmful-digital-communications-bill-

Although the Law Commission had recommended a new tribunal to deal with cyber bullying complaints, this has not been included in the draft legislation introduced in parliament. Rather, an approved agency is the first port of call under the legislation, with the district court empowered to issue remedies such as take-down orders and cease-and-desist notices.

The acting justice minister highlighted the safe harbour provisions of the bill, noting that any content hosts and websites will not be liable for unlawful content that another person has posted on the website unless they are notified that the content is unlawful and fail to take reasonable steps to remove the content.

At the first reading, both the Green and Labour parties indicated their support for the bill, subject to the analysis of the Justice and Electoral Committee.[51]

The Justice and Electoral Committee received 48 submissions of review of the bill from members of the public and private sector, including from Microsoft, Vodafone, Facebook, Yahoo and Google.[52]

## 4.4. Recourse available through the act

There are two primary implications of the bill for victims of online harassment seeking recourse: a civil enforcement regime, and the establishment of new criminal offences.

***Civil enforcement regime***

The bill sets out 10 new communication principles to guide the functions of the court and the approved agency that is set up under the legislation to receive and assess complaints about harm caused to persons by digital communications. The 10 principles are as follows:

- A digital communication should not disclose sensitive personal facts about an individual (Principle 1).
- A digital communication should not be threatening, intimidating or menacing (Principle 2).
- A digital communication should not be grossly offensive to a reasonable person in the complainant's position (Principle 3).
- A digital communication should not be indecent or obscene (Principle 4).
- A digital communication should not be part of a pattern of conduct that constitutes harassment (Principle 5).
- A digital communication should not make a false allegation (Principle 6).
- A digital communication should not contain a matter that is published in breach of confidence (Principle 7).
- A digital communication should not incite or encourage anyone to send a message to a person with the intention of causing harm to that person (Principle 8).
- A digital communication should not incite or encourage another person to commit suicide (Principle 9).
- A digital communication should not denigrate a person by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability (Principle 10) (Part 1, Subpart 1, Clause 6).

%E2%80%94-first-reading

[51] Ibid.

[52] www.parliament.nz/en-nz/pb/sc/documents/evidence/?Custom=00dbhoh_bill12843_1&Criteria.PageNumber=1

The civil enforcement regime provides for initial complaints about harmful digital communications to be made to an approved agency, which may investigate and attempt to resolve the complaint by negotiation, mediation and persuasion. If they cannot resolve the complaint, an individual may make an application to the district court for a number of civil orders, including:

- Requiring harmful digital communications to be taken down
- Requiring the defendant to cease the harmful conduct
- Ordering the identity of the author of an anonymous communication to be released.

The court may also make a declaration that a communication breaches a communication principle. The court will have jurisdiction over all forms of digital communication, and be able to use an expert technical adviser to ensure any remedies are technically achievable and appropriate. However, the safe harbour provisions do not apply if a content host does not provide an easily accessible mechanism for users to report such content to them.

***Criminal offences***

The law also creates a number of new offences. In addition to the offence of failing to comply with an order of the court (for which the maximum penalty is a fine of NZD 5,000 for an individual and NZD 20,000 for a body corporate), the bill creates the following offences to deal with the most serious forms of harmful digital communications:

- An offence of posting a harmful digital communication with the intention to cause harm (for which the penalty is imprisonment not exceeding three months, or a fine not exceeding NZD 2,000).
- An offence in the Crimes Act of inciting a person to commit suicide where suicide has not been attempted.

***Safe harbour provisions***

The HDCB also clarifies the law relating to the civil and criminal liability of internet intermediaries hosting content posted by third parties. The bill stipulates that a content host cannot be held liable for content which they do not know about unless they receive notice of a complaint about the content and fail to take reasonable steps to remove it.

***Amendments***

The HDCB also serves to amend a number of other acts, including:

- *Harassment Act 1997* – The HDCB amends the definition of harassment to include a single continuing act that is carried out over a protracted period, and to include electronic communications in the definition of a specified act.
- *Human Rights Act 1993* – The HDCB amends the act to include references to the use of electronic communications, and to expand the situations to which the sexual and racial harassment provisions apply to include when a person participates in a forum for the exchange of ideas and information.
- *Privacy Act 1993* – The HDCB amends the act to limit the public availability exception to the use of personal information so that it applies only if it would not be unfair or unreasonable to use or disclose the information.

## 4.5. Analysis and critique

***The penalisation of online speech***

Concerns expressed by some of the submissions made to the Justice and Electoral Committee related to the penalisation of behaviour that would not be unlawful offline. Such concerns were raised in submissions by Google and Microsoft, for example, but also by digital rights organisation Tech Liberty. The latter submitted that the bill would result in online and electronic communications being held to a different and higher standard than offline speech, and that the bill posits that harming someone through a digital communication is somehow worse than a comparable level of harm done through another form of communication.

The Tech Liberty submission bears replication here in part:

> This Bill seems to take the view that harm, defined as serious emotional distress, is to be avoided wherever possible. That speech which causes such harm should be limited and controlled, with the speaker restrained and punished. Oddly, the Bill only applies this principle of "no serious emotional harm" to speech communicated electronically. For example, harmful speech must be limited and stopped if it is communicated by text message, radio waves, television or the internet. Harmful speech communicated by voice, newspaper, billboard or letter will have a completely separate set of rules with no agencies to help mediate, and no quick fire court action.
>
> The absurdity of this distinction becomes plain when you consider the content of a "poison pen" note written on paper and slipped under the door. This Bill would not take any notice of the possible harm caused by this non-digital communication – unless someone then took a photo of it and emailed it.
>
> We acknowledge that some argue that electronic speech is different because it can spread faster or can be more easily distributed. We do not deny that people use the internet and other digital services to be horrible to each other. But at the same time, we have lived with rumour, gossip, anonymous letters, scurrilous posters and the consequent harms for many years. This sort of cruelty, and the suffering it can lead to such as social ostracism or suicide, sadly seems to be inherent to being human. At the same time, the internet has empowered new ways to counter such harm, empower victims and for society to condemn perpetrators of such cruelty.[53]

The Tech Liberty submission raised some interesting and challenging issues, particularly regarding the double standards between online and offline communications. However, it failed to deal with the nature of crowd mentalities, and the speed and reach of communications that are aggravated in anonymous digital communications.

In contrast, the New Zealand Human Rights Commission submitted that it believed the bill strikes the correct balance between freedom of expression and access to the internet.[54]

***Effectiveness and implementation***

There are concerns that a civil enforcement regime is unlikely to provide quick and effective remedy for users of digital communications. This was highlighted during the first reading of the bill by the opposition

[53] Tech Liberty. (2014, February 21). Submission: Harmful Digital Communications Bill. *Tech Liberty*. techliberty.org.nz/submission-harmful-digital-communications-bill
[54] www.parliament.nz/resource/0002218170

party, who drew a comparison with the Victims' Orders Against Violent Offenders Bill that is also dependent on civil action. It was argued that, under such regimes, the victim has to meet the cost of dealing with something that, actually, the criminal justice system and the state might be better equipped to deal with.

There is an additional barrier to effectiveness given that many of the orders that a court will be empowered to make under the legislation will be difficult to enforce in a cross-jurisdictional context.

***Failure to gain the input of women's organisations***

A submission by Tech Liberty highlighted that although a significant rationale for the bill (cited in Cabinet Papers and the Law Commission papers) is the need to address cyber bullying and violence against women, there are serious concerns that the bill has been drafted without meaningful input from women's organisations.[55] In its submission to the Justice and Electoral Committee, the National Council of Women of New Zealand expressed particular concern about the establishment of a new agency, calling on the government to ensure that the education and experience of the appointees should be appropriate, the appointees should have good ethical standards, legal knowledge, expertise in mediation, social media and information technology and be free of prejudice.[56] There were also comments that the appointees should be from a good cross-section of the community to ensure gender, age, socioeconomic and cultural balance.[57]

## Conclusions and comparative analysis

In a general sense, the four pieces of legislation analysed above represent a clear trend at the domestic level for parliaments to seek to create new avenues of redress for the increasingly prevalent problem of technology-related violence, particularly as it affects women and children. Beyond that, the acts highlight the emergence of interesting attitudes and approaches, which we have sought to identify below:

1. **The need to provide practical avenues of redress**
   Each of the acts has as its primary objective the creation of a practical form of redress for actions that were not previously cognisable within the criminal or civil law frameworks. Importantly, all of the legislation recognises that harm caused by harassment online includes emotional distress, even if there is no actual physical harm. The South African and Nova Scotian acts provide for a system of protection orders, a simple, effective and efficient form of getting immediate recourse against an individual perpetrating harassment or bullying. The New Zealand system provides for a civil enforcement regime where behaviour does not comport with a set of communication principles prescribed by the act. The Californian and New Zealand regimes provide for new criminal offences related to harmful behaviour online. The South African, Nova Scotian and New Zealand legislation all provide for various forms of criminal offences related to non-compliance with court orders. Each of these provisions allows for a victim of online harassment, violence or bullying to achieve concrete redress or change, an important aspect of accessing justice.

[55] Tech Liberty. (2014, February 21). Op. cit.

[56] For a critical analysis of the proposed agency, see: Liddicoat, J. (2013). Proposed new laws and their impact on women. En A. Finlay (Ed.), *Global Information Society Watch 2013*. Johannesburg: APC and Hivos. www.giswatch.org/en/country-report/womens-rights-gender/new-zealand

[57] www.parliament.nz/resource/0002202418

2. **The imposition of responsibility on communications intermediaries**
   The South African, Nova Scotian and New Zealand legislation all reflect the increasing need for internet and communications intermediaries to play a role in preventing and rectifying online violence, harassment and bullying. The legislation recognises that electronic communications often facilitate anonymity, which can be a barrier to accessing justice for violence against women online. It therefore places a burden on electronic service providers to respond to requests for information about the identity of the harasser (in South Africa and Nova Scotia), to cease providing service upon the order of a court (in Nova Scotia) and even to remove offensive content when service providers become aware of its presence on their sites (New Zealand). In South Africa, an individual within a company, as well as the company itself, can bear criminal liability for failing to comply with a court's request to facilitate the identification of an individual accused of online harassment.

3. **Free expression implications**
   In the passage of the legislation in California, Nova Scotia and New Zealand (ongoing), there have been arguments raised about the implications for free speech. In each case, these arguments have had a slightly different nuance. In Nova Scotia, the concerns raised have related to the broad powers of a court to prevent internet access or confiscate technologies; in California, initial opposition of the amendment resulted in a considerable narrowing of the offence to apply only where there was an agreement between parties that the image was to remain private. The free expression implications are perhaps the most significant in the case of New Zealand – the proposed legislation seeks to "civilise" online communications by preventing, for example, grossly offensive, indecent or obscene digital expression. In doing so, the legislation seeks to apply different standards to online communication and expression than to offline communication and expression. On one hand, the legislation recognises the unique nature of digital communications – the speed with which they are promulgated and proliferate, the inability to permanently erase them, and the insulating nature of anonymous communications that can promote an offensive of violent behaviour. The fact that the potential for harm can be attributed differently to digital technologies than offline speech is seen as a basis for treating electronic communications differently.[58] On the other hand, however, the legislation also applies a number of subjective and general standards to all digital communications, which, depending on a court's interpretation, could be applied in ways that limit free expression and could undermine the free flow of information.

4. **The need to accompany legislative changes with public education**
   Critics across these contexts have suggested that legislation alone cannot solve the problem; and that any legislative changes must be accompanied by public awareness and education campaigns on the gendered nature of harm in digital spaces, issues of consent, as well as awareness of what actions constitute criminal offences and the possibilities for liability. Especially when youth may be the "offenders", or parents may be held liable for the actions of their children, resources need to be put towards initiatives that bring the spirit of the law into public education. The Nova Scotian process highlights a positive approach in this regard: ensuring a budget increase of CAD 900,000 towards resources for survivors of sexual violence, as well as coordinating a provincial education campaign on cyber bullying.

An analysis of the legislative history and application of these four acts also suggests some positive elements that could provide a useful starting point for other legislatures seeking to amend legal frameworks to make them more hospitable to complaints of technology-related violence. Some of these

[58] Anita Gurumurthy, peer review on the paper in an email to APC, 8 June 2014.

elements include:

- **A consultative process**
  The use of a consultative process in designing the South African legislation – which extended over multiple years and allowed for actors from a range of positions to provide feedback on the bill – helped to build widespread support for the legislation. This can be contrasted with the experiences in Nova Scotia and California, where bills were rushed through the legislature without first gaining widespread public buy-in.

- **Utilising/amending existing legal frameworks vs. creating new laws**
  The South African experience again provides a valuable template. After doing an extensive review of existing laws, the Law Reform Commission concluded that existing criminal laws could sufficiently cover crimes related to harassment online; what was needed was a redress process which would allow for immediate relief. This experience can be contrasted against the New Zealand example, where the legislation proposes wholesale change to the regulatory framework and the imposition of a new regime, and the Nova Scotian act, which creates new categories of crimes. The adequacy and efficacy of these different routes for providing redress remains to be seen. For example, has the enlarged definition of harassment extending to online spheres been adequately understood and applied under the South African law? Or will a different perspective specifically covering electronic mediums be necessary? In practice, has the application of the Nova Scotian, New Zealand and Californian legislation resulted in the curtailing of individual rights as some opponents feared? Further research to this end could be a valuable lesson for advocates in other contexts.

- **Focus on redress over criminalisation**
  While the option of criminal law recourse may indeed have a distinct purpose, the Nova Scotia, South Africa and New Zealand acts all focus on redress and relief over criminalisation. This seems to be the most effective, efficient and meaningful way of aiding victims of violence online and ensuring that justice is achieved. The use of protection orders to address technology-related violence against women is an important advancement that should be considered in other jurisdictions. Protection orders are used in many countries to address domestic violence, by providing a practical means of halting violence without requiring victims to become embroiled in lengthy and demanding criminal processes. Although the effectiveness of protection orders in the context of online harassment remains to be seen, it is a novel application of a method that has seen success in other domains.

- **Creating a dedicated agency to receive and investigate complaints**
  Both Nova Scotia and New Zealand propose to create a dedicated agency to receive and investigate complaints made under new legislation. Although the New Zealand legislation has not yet been adopted, in Canada the establishment of the CyberSCAN unit has been met with approval and seems to be experiencing success, with scores of claims having been received, mediated and resolved over its short lifespan.

- **Impact of public campaigning**
  The passage of each of the domestic acts is testament to the power of public awareness raising and campaigning in achieving legislative change. Although each of the acts followed a high profile event that created motivation for swift legal change, they also benefited from the work of public advocacy groups who seized on the momentum, built public awareness and created impetus for legislative change.

ISBN: 978-92-95102-29-3
APC-201405-WRP-R-EN-DIGITAL-220