Australian Human Rights Commission

Background paper: Human rights in cyberspace

September 2013

Australian Human Rights Commission
www.humanrights.gov.au

Contents

1 Background and context

The Internet has been in existence since the 1960s, and the World Wide Web since the 1990s.[1] Cyberspace, however, remains a relatively new terrain in terms of the questions it raises about human rights and responsibilities.

The International Telecommunication Union estimates that almost 40% of the world's population, and over 76% of people in developed countries, are now internet users.[2] Government, businesses, and organisations in civil society are increasingly using cyberspace platforms in the communication of information and the delivery of services. More than any previous communication medium, the Internet also offers individuals the ability to be active publishers of information on a large scale, rather than only recipients.

Accordingly, the Internet has become a major vehicle for the exercise of the right to freedom of expression and information.

The *International Covenant on Civil and Political Rights* (ICCPR)[3] states (in article 19(2)):

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

The United Nations Human Rights Committee (HRC) has provided extensive commentary on this article in its *General Comment number 34: Freedoms of opinion and expression*.[4] The HRC has stated that the freedoms of expression and information under article 19 of the ICCPR include the freedom to receive and communicate information, ideas and opinions through the Internet.[5]

Article 19(3) provides that:

> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

This means that (like many other rights) the right to freedom of information must be balanced with other rights.[6] The UN Human Rights Council has stated that 'the same rights that people have offline must also be protected online' (mentioning in particular freedom of expression).[7]

Laws seeking to balance rights and responsibilities often distinguish between public and private conduct. The rapid development of the Internet in terms of its use in daily life has blurred these lines.

People are increasingly using the Internet for activities that they would perceive to be 'private' communications (i.e. staying in touch with friends, family, social groups). However, defamation law, for example, requires only that a person be identified in material which is established to be defamatory, and that the material be 'published' (communicated to someone other than the aggrieved person).

'Publishing' can no longer be thought of as restricted to traditionally off-line mediums such as newspapers, television, radio broadcasts, books, posters or handbills. Arguably every time anything is posted on the Internet it constitutes an act of 'publication' for the purposes of defamation.

One question is: are people's expectations of privacy different in cyberspace because they are using an online medium, or does it depend on the context?

Anti-discrimination laws identify and apply to specified areas of 'public life' (e.g. employment; accommodation; education; provision of good and services). These areas have themselves been rapidly expanded by the use and application of the Internet in employment and education, as well as in the delivery of goods and services.

But what about activities which do not necessarily fall within a public area in themselves, but might be considered public because they are conducted through the Internet?

In the case of discrimination conducted through the Internet, even where 'public' behaviours are identified, there is a question whether the person or people responsible can be identified. Further, how can rules in anti-discrimination or other laws be enforced in relation to conduct on the Internet where there are questions about where the act complained of occurred?

The premise of this paper is that the creation of the Internet has not unleashed a set of 'new behaviours' – rather it largely reproduces pre-existing behaviours within an online medium. What has changed is the impact of these behaviours, and challenges regarding the regulation of such behaviours.

2 Scope of this paper

This paper is intended to contribute to discussion; it is not intended to comprehensively or conclusively cover all issues surrounding human rights in cyberspace. The Australian Human Rights Commission (Commission) has worked and continues to working on a range of human rights issues connected with the Internet, including

- access and accessibility for people with disability
- access and online safety for older Australians
- racial discrimination and vilification in online environments
- sexual harassment over the Internet
- cyber safety for children and cyber-bullying
- online safety in Indigenous communities

The Commission's has also been conducting a series of 'RightsTalks' seminars on human rights and the Internet. Links to the full range of activities by the Commission on issues of human rights and cyberspace are available on our project page on human rights and the internet.[8]

In this paper three issues in particular are raised for consideration:

- freedom of expression and Internet censorship
- effective responses to racism, sexism, sexual harassment and homophobia on the Internet
- rights to access the Internet.

3 Freedom of expression and the Internet

The Internet has opened up new possibilities for the realisation of the right to freedom of expression. This is due to the Internet's unique characteristics, including 'its speed, worldwide reach and relative anonymity'.[9] These distinctive features have enabled individuals to use the Internet to disseminate information in 'real time', and to mobilise people.[10] The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Special Rapporteur) asserts that:

> Unlike any other medium the Internet facilitated the ability of individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an 'enabler' of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole.[11]

Insofar as freedom of expression is concerned, the Internet presents a compelling platform for the decentralising of information and of institutional control – at its best it acts as a leveller to access to knowledge.

However, as the Special Rapporteur acknowledges, 'like all technological inventions, the Internet can be misused to cause harm to others.[12]

3.1 Freedom of expression in human rights theory

The right to freedom of expression is deeply rooted in historical thought and underpinned by a number of largely interdependent rationales.

Of these is the 'truth rationale' where 'true opinion' can be identified, and 'false ideas' exposed through criticism – a process facilitated by a free-flowing 'marketplace of ideas'.[13]

The 'democratic rationale' identifies freedom of expression as necessary for the functioning of a truly representative government.[14] The HRC has emphasised the importance of press and media freedom for a democratic society:

> A free, uncensored and unhindered press or other media is essential in any society to ensure freedom of opinion and expression and the enjoyment of other Covenant rights.

> It constitutes one of the cornerstones of a democratic society. … The free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion. The public also has a corresponding right to receive media output.[15]

A core rationale for freedom of expression is the 'self-determination rationale', in which free speech is conceived of as an aspect of self-realisation and individual autonomy.[16] The ability to relate our thoughts and experiences is seen as an intrinsic part of being human, and therefore restrictions on this ability are viewed as inhibiting both individual autonomy and the ability to attain self-fulfilment.

In this vein, the HRC has also noted that freedom of information and expression, while central to democratic governance, is not restricted to political information and expression; it

> includes the expression and receipt of communications of **every form of idea and opinion capable of transmission to others**, subject to the provisions in article 19, paragraph 3, and article 20. It includes political discourse, commentary on one's own and on public affairs, canvassing, discussion of human rights, journalism, cultural and artistic expression, teaching, and religious discourse. It may also include commercial advertising.[17]

Accordingly, the right to freedom of expression has been described as an 'enabler of other rights' such as economic, social and cultural rights (i.e. rights to education and to take part in cultural life) as well as civil and political rights (i.e. rights to freedom of association and assembly).[18]

3.2 Freedom of expression and information in Australian law

In Australia there is no express Constitutional or legislative protection of the freedom of expression at the federal level (in contrast to human rights legislation in force in the ACT and Victoria),[19] Despite this, the courts have an important role in interpreting legislation consistently with human rights where possible.[20]

Although not expressly protected at a federal level, freedom of expression does enjoy some implied and residual[21] protection. The Australian High Court has held that an implied freedom of political communication 'is an indispensable incident of the system of representative government which the Constitution creates'. [22]

The freedom of political communication found by the High Court to be implicit in the Constitution is unlikely to have the same breadth of subject matter as article 19(2) of the ICCPR, insofar as the latter goes beyond political matters. However, the very fact of restrictions being placed on freedom of expression on other subjects – including on grounds such as decency - may in some instances itself give the restricted or prohibited expression the status of political communication.

A number of potential restrictions on the right to freedom of expression are contemplated by Australian laws, including in laws on sedition;[23] national security;[24] telecommunications;[25] racial hatred;[26] copyright;[27] defamation;[28] perjury;[29] contempt of court;[30] fraud;[31] privacy,[32] and censorship in classification and broadcasting.[33]

A number of these laws are based on valid grounds for restriction referred to in article 19(3) of the ICCPR. However, questions remain as to whether some of these laws would meet the levels of transparency and proportionality required by article 19(3).

These questions raise broader concerns about censorship and the Internet. In particular, the Special Rapporteur notes the use of arbitrary blocking or filtering of content where such mechanisms are used to regulate and censor information on the Internet, with multi-layered controls that are often hidden from the public.[34] An example of such a system close to home was the Australian Government's now discontinued mandatory Internet filtering proposal. This attracted wide-ranging criticism as providing broad and imprecisely defined parameters on what constituted 'refused classification' materials, resulting in websites being captured by the filter which were described by critics of the proposal as relatively innocuous.[35]

As the Special Rapporteur points out, excessive censoring can occur where the specific conditions that justify blocking are not established in law or are legislated for in an 'overly broad and vague manner'.[36] In addition, even where justification for blocking exists, blocking measures may constitute a disproportionate means to achieving the purported aim, and content may frequently be blocked without the possibility of judicial or independent review.[37] This situation requires the balancing of freedom of expression against other rights and considerations that should be taken into account in achieving the appropriate balance.

3.3 Right to freedom of expression and information in human rights instruments

'Human rights' for the purposes of the Commission's work include the rights and freedoms recognised in the ICCPR, including the right to freedom of expression and information in article 19. As discussed on the Commission's webpage on the right to freedom of information, opinion and expression,[38] this right is also recognised and expanded on in the *Convention on the Rights of the Child* (CRC)[39] and the *Convention on the Rights of Persons with Disabilities*.[40] Freedom of expression and information is also recognised in article 19 of the *Universal Declaration of Human Rights*.[41]

The following discussion will focus on the right to freedom of expression as recognised by article 19 of the ICCPR.

4 Permissible limitations of the ICCPR right to freedom of expression

As noted above, article 19(3) of the ICCPR permits limitations on the rights recognised in article 19(2), but those limitations must be:

(1) provided by law and

(2) necessary for respect of the rights or reputations of others, for the protection of national security, public order, or public health or morals.

The HRC in its *General Comment 34* has emphasised that:

> when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself…the relation between right and restriction and between norm and exception must not be reversed. [42]

Australia's Joint Parliamentary Committee on Human Rights has similarly made the point that:

> Given the fundamental nature of this right, international human rights bodies have scrutinised with great care any limitations on freedom of expression, including the introduction of regulatory schemes for media. They have insisted that States demonstrate convincingly the need for measures which prevent or restrict the operation of a free and independent media, and have been especially concerned about content-based restrictions and restrictions which might inhibit the expression of views that contribute to public and political debate. [43]

The HRC further stated that:

> Paragraph 3 lays down specific conditions and it is only subject to these conditions that restrictions may be imposed: the restrictions must be "provided by law"; they may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3; and they must conform to the strict tests of necessity and proportionality…Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated.[44]

4.1 Provided by law

The requirement for limitations regarding freedom of information and expression to be 'provided by law' is an important guarantee of the rule of law. It includes a formal requirement of legality - that is, that there be a legal basis for restrictions. It also includes substantive requirements. The HRC has noted:

> For the purposes of paragraph 3, a norm, to be characterized as a "law", must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not. [45]

4.2 Permissible purposes[46]

(a) Respect for the rights or reputations of others

Article 19(3) provides that freedom of expression may be limited where those limitations can be demonstrated to be necessary for ensuring 'respect for the rights and reputations of others'.

A range of rights may present possible justifications for limitations on freedom of expression through the internet, including:

- freedom from discrimination (article 2 of the ICCPR)
- freedom from cruel, inhuman or degrading treatment (article 7 of the ICCPR and article 37(a) of the CRC)

- the right of children to special protection (article 24 of the ICCPR and article 3 of the CRC)
- freedom from arbitrary interference with home, family, correspondence or reputation privacy (article 17 of the ICCPR).

Whether particular restrictions on freedom of expression which are designed to protect these rights are justifiable will depend on more specific consideration of the restrictions concerned and the circumstances.

(i) Freedom from discrimination

Article 2(1) of the ICCPR requires parties to ensure the rights contained in that covenant to all individuals 'without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.' Article 2(2) of the *International Covenant on Economic, Social and Cultural Rights* (ICESCR)[47] is to similar effect.

In addition, article 26 of the ICCPR states that:

> the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Article 20 of the ICCPR further states that '[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.' It should be noted that Australia has made (and maintains) the following interpretative declaration and reservation regarding article 20:

> Australia interprets the rights provided for by articles 19, 21 and 22 as consistent with article 20; accordingly, the Commonwealth and the constituent States, having legislated with respect to the subject matter of the article in matters of practical concern in the interest of public order (*ordre public*), the right is reserved not to introduce any further legislative provision on these matters.

The HRC has similarly indicated that article 20 of the ICCPR is required to be interpreted consistently with article 19:

> Articles 19 and 20 are compatible with and complement each other. The acts that are addressed in article 20 are all subject to restriction pursuant to article 19, paragraph 3. As such, a limitation that is justified on the basis of article 20 must also comply with article 19, paragraph 3.[48]

The principal provision in federal law which is intended to address the requirements of article 20 of the ICCPR is s 18C of the *Racial Discrimination Act 1975* (Cth) (RDA). Section 18C provides:

> (1) It is unlawful for a person to do an act, otherwise than in private, if:
>
> (a) the act is reasonably likely, in all the circumstances, to offend, insult, humiliate or intimidate another person or a group of people; and
>
> (b) the act is done because of the race, colour or national or ethnic origin of the other person or of some or all of the people in the group.

However, the application of s 18C of the RDA is subject to a wide range of exceptions (set out in s 18D) for things said or done reasonably and in good faith.

The protection against discrimination which is required by articles 2 and 26 of the ICCPR includes a broader range of grounds than are currently covered by any vilification provisions (such as 18C) under Australian anti-discrimination law. Any further legislation to implement articles 2 and 26 which restricted the right to freedom of expression would have to meet the requirements of ICCPR Article 19(3), including the requirements of necessity and proportionality.

In order to avoid impermissible limitations of the right to freedom of expression and information, particular caution would be required in the design and administration of any provisions addressing vilification on the basis of religion or belief. The Human Rights Committee has indicated:

> Prohibitions of displays of lack of respect for a religion or other belief system, including blasphemy laws, are incompatible with the Covenant, except in the specific circumstances envisaged in article 20, paragraph 2, of the Covenant.[49]

(ii) Freedom from cruel, inhuman and degrading treatment

Article 7 of the ICCPR provides that '[n]o one shall be subject to torture or to cruel, inhuman or degrading treatment or punishment.' The right to be free from the types of ill-treatment listed in article 7 is not confined to actions affecting people in prison, in detention or in institutional environments; nor is it confined to actions by or on behalf of the State itself.

The Commission's strategic priorities include violence, harassment and bullying.[50] Bullying in particular can be regarded as conduct (in whatever context) which could in more technical terms be referred to as 'cruel', 'inhuman' or 'degrading'.

The specific right of children to be free from cruel, inhuman or degrading treatment is recognised in article 37(a) of the CRC. The Committee on the Rights of the Child has described cruel inhuman or degrading treatment in relation to children as including treatment which 'belittles, humiliates, denigrates, scapegoats, threatens, scares or ridicules the child.'[51]

Any measure which is designed to protect children from being bullied over the Internet needs to balance:

- the CRC's interpretation of the right to protection from cruel, inhuman or degrading treatment (which the Commission endorses in relation to children), and
- the rights to freedom of expression and information (including for children- see article 13 of the CRC), and the requirement that any restrictions of those rights be provided by law and necessary and proportionate.

(iii) Right of children to special protection

Higher levels of restrictions on the right to freedom of expression and information, as engaged by conduct affecting *children,* may be justifiable having regard to the rights of children to special protection under the CRC.

Article 24 of the ICCPR states that children are entitled to necessary measures of protection, on the part of their families, society and the State. Article 3(2) of the CRC requires States parties to ensure for children such care and protection as is necessary for their well-being, and take all necessary legislative and administrative measures to achieve this.

In this regard, article 17 of the CRC, which recognises the importance for children of access to information and material through the mass media, requires States parties to (among other things):

> Encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of articles 13 [freedom of information and expression] and 18 [recognition of responsibilities of family].

In summary, while restrictions on access by children to some material on the Internet may be permissible (and in fact regarded as required), governments applying such restrictions are nonetheless required to justify with regard to the criteria for permissible limitations of the right to freedom of expression.

(iv) Right to privacy, family, home, correspondence, honour and reputation

Article 17 of the ICCPR states that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The HRC has indicated its view that 'this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons.'[52]

However, the Committee has also observed that '[a]s all persons live in society, the protection of privacy is necessarily relative.'[53] Balancing the rights to privacy and/or protection of reputation with the rights to freedom of information and expression presents challenges. It is clear however that measures to protect these rights which limit freedom of expression and information must comply with the requirements set out in article 19(3) of the ICCPR.

(b) Public morals

Respect for "public morals" is a permissible justification for restricting the right to freedom of expression and information, subject to compliance with the conditions provided in 19(3) of the ICCPR. In its *General Comment No. 34*, the HRC stated:

> The Committee observed in general comment No. 22, that "the concept of morals derives from many social, philosophical and religious traditions; consequently, limitations... for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition". Any such limitations must be understood in the light of universality of human rights and the principle of non-discrimination.[54]

As noted earlier, restrictions on this ground are also required to be sufficiently precise to comply with the requirement that restrictions be 'provided by law'.

(c) Public order

Article 19(3) permits restrictions aimed at protecting public order (*ordre public*). The Commission has noted that this concept:

> is clearly wider than the concept of 'public order' in the sense usually understood in Anglo-Australian law (dealing with prevention of breaches of the peace, offensive behaviour etc). It extends to the sum of rules which ensure the functioning of society or the set of fundamental principles on which society is founded. It equates with the 'police power' in United States jurisprudence, permitting regulation in the interests of legitimate public purposes. This power must itself, however be exercised in a manner consistent with human rights.[55]

Restrictions on promotion of unlawful activity would appear to be permissible under this heading (subject to the requirements of necessity and proportionality being met). The HRC has considered this point specifically in relation to counter-terrorism measures such as offences of "encouraging", "praising" or "justifying" terrorism.[56]

4.3 Restrictions must be 'necessary' for a permitted purpose

The HRC has made clear its view that the requirement under article 19(3) that a measure limiting freedom of information and expression be 'necessary' imposes a substantial burden of justification on government agencies. It has stated that this equates to a requirement that any 'restrictive measures must conform to the principle of proportionality':

> they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected …The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law. The principle of proportionality must also take account of the form of expression at issue as well as the means of its dissemination. For instance, the value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain.[57]

The HRC further stated that:

> When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat.[58]

5 Current issues of 'Internet censorship': bullying, discrimination, harassment and freedom of expression

The Australian media has increasingly reported on a wide-range of issues relating to forms of Internet censorship, including tracing Internet-based child pornography

rings; calls to shut down racist memes[59] sites; courts ordering the removal of Facebook hate pages involving suspects of crimes; or calls to regulate bullying or offensive behaviours.

Unsurprisingly, discriminatory behaviours that occur 'off-line' in everyday life, also occur 'online'. The Commission's statutory responsibilities regarding discrimination and protection of human rights have required the Commission to focus on behaviours involving the Internet such as cyber-bullying and online racism, sexism/sexual harassment and homophobia.

5.1 Cyber-bullying

Perhaps the most well-known 'cyber' form of offensive behaviour is 'cyber-bullying'. Cyber-bullying can be defined as a person (or a group of people) using technology to repeatedly and intentionally use negative words and/or actions against a person, which causes distress and risks that person's wellbeing.[60] In June 2010 young people aged 14 -17 years old had the highest rate of Internet use in Australia, with 91% spending time online every week.[61] Cyber-bullying affects at least one in ten students in Australia.[62]

Cyber-bullying can impact on a range of human rights, including:

- The right to the highest attainable standard of physical and mental health:[63] Bullying can impact negatively on a person's physical and mental health causing harm in the form of physical injuries, stress-related illnesses, depression and other health issues.
- Rights to work and fair working conditions:[64] Bullying can lead to higher absenteeism from the workplace, poor or reduced performance and an unsafe working environment.
- The right to freedom of expression and to hold opinions without interference:[65] Bullying can impact on a person's freedom to express feelings or opinions as they no longer feel safe to do so.
- A child or young person's right to leisure and play:[66] Bullying often occurs where children and young people play and socialise, such as in school playgrounds and on social networking sites. All children have the right to participate in leisure activities in a safe environment. The United Nations Committee on the Rights of the Child, in its report on Australia's compliance with the Convention on the Rights of the Child, raised concerns about bullying and the importance of protecting children and young people from exposure to violence, racism and pornography through mobile phones and other technologies, including the internet.[67]
- The right to an education (as cyber-bullying it can make a person feel unsafe and unwelcome at school and impact on how well they do).[68]
- The right to be free from violence, whether physical or mental.[69]

5.2 Cyber-racism

There are many examples of cyber-racism on the Internet, from racist individual Facebook posts to group pages specifically set up for a racist purpose. An example

of cyber-racism that gained considerable media notoriety was an Aboriginal memes Facebook page that consisted of various images of Indigenous people with racist captions.[70] It was reported that Facebook had classified this memes page as 'controversial humour' despite the fact it was said to have depicted an entire race of people as 'inferior drunks who sniff petrol and bludge off welfare'.[71] It was further reported that while the creators of the page had ultimately removed the content, Facebook had not deleted the actual page (still classified as 'controversial humour').[72]

5.3 Cyber-sexism/sexual harassment

Instances of cyber-sexism are similarly numerous. The Commission's Workplace Sexual Harassment Survey of 2012 revealed that 17% of those surveyed had been in receipt of sexually explicit emails and text messages and 4% had experienced repeated/inappropriate advances on email, social networking websites and internet chat rooms.[73] Other examples of cyber-sexism/sexual harassment include 'creep-shots' where men take pictures of intimate body parts of unsuspecting women snapped on the street and load them on to a publicly accessible website.[74] Another instance of cyber-sexism, which was subject to an online petition, was a page that published photos of young girls posing in pictures that had already been posted on the social media site on their own pages.[75] The pictures were then branded with lewd tags and posted on a page entitled '12-year old sluts'.[76]

5.4 Cyber-homophobia

The incidence of homophobic cyber-bullying has increased greatly in recent years with the proliferation of online social networking tools.[77] A homophobic language 'audit tool' has been developed that measures in real time when certain homophobic words are used on Twitter, and keeps a record so that usage can be measured over time. It demonstrates the high rates of 'casual' homophobic language used in every day interactions on Twitter and how common their usage has become.[78]

There have been high profile cases of LGBTI young people being bullied and harassed online that have resulted in self-harm and suicide.[79] A much publicised US case on the use of technology in homophobic bullying involved a university student who killed himself shortly after discovering that his roommate had secretly used a webcam to stream his sexually intimate actions with another man over the Internet.[80]

As highlighted by the examples listed above, it is clear that the Internet is being used in different ways to facilitate various forms of discrimination and harassment. This raises the question: how do Australian laws respond to and regulate these behaviours?

6 Some regulatory challenges

6.1 Balancing of rights

The challenge of finding the appropriate balance between rights is not one which is specific to the Internet.

It is difficult to know if Australian laws that limit freedom of expression in the interests of other rights, or on other permissible grounds, have 'drawn the line' appropriately without a comprehensive review of such laws. In New Zealand, a legislative review undertaken by the New Zealand Law Commission indicated that 'much of the law is expressed in terms of flexible principle which is technology-neutral and which can work perfectly well in the new environment'.[81] But even if these laws cover cyberspace, the question may still remain whether they allow for an appropriate balancing of rights.

From a human rights perspective it is clear that any limitation should be assessed against the criteria specified for permissible limitations in article 19(3) of the ICCPR.

In looking at, for example, the balance between protecting freedom of expression and prohibiting advocacy of racial hatred, some critics have argued that the vilification provisions contained in s 18C of the RDA set the threshold for the limitation on free speech too low.[82] Others argue that to read s 18C in isolation from the exceptions in s 18D fails to recognise that freedom of expression is adequately protected.

While debates will continue as to what is the 'appropriate balance' between freedom of speech and other rights, it should be asked, how does cyberspace change the equation – if at all? It is arguable that while the types of behaviours which people engage in online are not new, what has changed is the way these behaviours are manifested online, and consequently the impacts of these behaviours. As the New Zealand Law Commission noted:

> For the first time in history, individuals with access to basic technology can now publish, anonymously, and with apparent impunity, to a potentially mass audience. This facility to generate, manipulate and disseminate digital information which can be accessed instantaneously and continuously is producing types of abuse which have no precedent or equivalent in the pre-digital world.[83]

The New Zealand Law Commission summarised the additional regulatory challenges presented by the Internet as:

- the viral nature of cyberspace and the potential for information to be disseminated instantly to worldwide audiences
- the ubiquity of the technology which means communications are no longer constrained by time and place but can be accessed anywhere, anytime by anyone
- the persistence of information disseminated electronically
- the ease with which digital information can be accessed/searched and
- the facility for anonymous communication and the adoption of multiple online personae.[84]

These particular features of cyberspace have meant that even where laws are drafted in technology-neutral terms which would cover activities in cyberspace, enforcement challenges exist which in turn raises issues of where to 'draw the line'. These issues are further compounded by a lack of knowledge of the law and/or about the availability of redress on the part of both victims and enforcement officers.[85] These 'cyber-enforcement' challenges are considered in further detail below.

6.2 Permanency

The instant any material is published on the Internet, a 'snapshot in time' archive of the material is created and will remain 'cached' or stored and potentially accessible via web-searches on a likely permanent basis. This process also means the information is searchable and easily capable of duplication. This feature of the Internet can significantly undermine the utility of a court ordering the removal of material from the Internet.

For example, in 2012 a Deputy Chief Magistrate ordered that material on the Internet relating to man accused of murdering Jill Meagher be removed prior to his trial, as it was deemed to prejudice the administration of justice. The Deputy Chief Magistrate was reported as stating that while it had been argued that an order to suppress material about the suspect was futile given the 'anarchic nature' of the Internet, the court had to do its best to protect the administration of justice.[86] The Victorian Court of Appeal has acknowledged that:

> As observed by the High Court in *Dow Jones v Gutnick* once an item is on the internet it is 'available to all and sundry without any geographic restriction'…the immediate accessibility of such information…poses substantial challenges for the administration of justice.[87]

6.3 Ubiquity

Another of the unique characteristics of the Internet is the way it facilitates the instant and global dissemination of information. It is this feature in particular that renders the Internet a powerful tool for freedom of expression, resulting in the Internet being attributed with everything from increasing access to information and 'facilitating active citizen participation in building democratic societies',[88] to being the 'driving force in accelerating progress towards development in its various forms'.[89]

Yet with the advantages that global communication offers, also come disadvantages. This is most clearly illustrated by the problem of online defamation. The global reach and instantaneous nature of the Internet means that the potential repercussions of defamatory statements can be far more damaging to a person's reputation than statements published 'off-line'.

The Special Rapporteur argues the opposite view, citing the ability of the individual concerned to 'exercise his/her right of reply instantly to restore the harm caused'.[90] However, quite apart from the global damage to an individual's reputation and the variable value of a 'right to reply', the issue of permanency and 'caching' may mean that a 'right to reply' is of limited value if it is not cached in the same places that the original comment appears on the Internet. The effectiveness of 'take down notices' is also questionable where material is cached on the Internet.

6.4 Anonymity

A further (and related) issue raised by Internet communications is that of anonymity. The Internet offers users an unprecedented ability to communicate 'anonymously' and, if desired, set up multiple 'personae' or online identities.[91]

The ability to be anonymous online can have beneficial effects in terms of the realisation of the right to freedom of expression. As the Special Rapporteur states:

> throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously. The Internet allows individuals to access information and to engage in public debate without having to reveal their real identities, for example through the use of pseudonyms on message boards and chat forums.[92]

The Special Rapporteur points to instances where certain States have used popular social networking sites such as Facebook to identify and to track the activities of human rights defenders and opposition members.[93] A number of States are also introducing or modifying existing laws in order to increase their power to monitor the activities and content of Internet users without adequate safeguards against abuse (in terms of who is allowed to access personal data, what it can be used for, how it should be stored, and for how long).[94]

However, commentators have also noted that such anonymity can have a 'disinhibiting effect' where 'people end up saying and doing things online that they would never dream of doing face-to-face'.[95] As one academic describes it: 'people disconnect a little bit and forget that what they are doing is just a continuation of other forms of communication rather than something that is fundamentally different'.[96]

An example of this 'disconnect' is clearly highlighted in the recent media controversy over 'cyber-trolls' and 'anonymous abuse'.

The New Zealand Law Commission cited two examples of anonymous abuse. The first involved female students at Yale Law School, who sued those responsible for a sustained campaign of anonymous sexual harassment launched by a group of young males on the college admissions web forum.[97] The female students contended that the postings about them became 'etched' into the first page of search engine results on their names, costing them prestigious jobs and infecting their relationships with friends and family.[98]

The second example involved a 45-year-old British woman in the UK who became the target of abusive behaviour after posting supportive comments about an 'X Factor' contestant on her Facebook page.[99] Anonymous attackers responded by creating a false profile in her name using her picture to post explicit comments and vilifying her.[100] In a landmark case in June 2012, the High Court granted the woman a disclosure order to compel Facebook to reveal the IP addresses and account details of those responsible for posting the offensive content.[101]

It should be noted that not all so-called 'cyber-trolls' engage in abusive behaviour, although they usually maintain anonymity as 'trolling is a game about identity deception'.[102] Cyber-trolls are diverse in their aims - some may wish to join a group with the intention of swaying opinions and to sow fear, uncertainty and doubt within the group, or more generally simply to provoke an argument. [103] While these behaviours can be annoying and unpleasant, they do not necessarily always amount to conduct which would clearly justify a limitation of the 'troll's' right to freedom of expression.

The HRC has noted that article 19(2) of the ICCPR 'embraces even expression that may be regarded as deeply offensive, although such expression may be restricted in accordance with the provisions of article 19, paragraph 3 and article 20.'[104] Accordingly, many unpleasant behaviours may be entirely consistent with cyber-trolls' right to freedom of expression. But where the actions of cyber-trolls contravene domestic laws and/or are a recognised limitation to the right to freedom of expression, the issue of their anonymity becomes challenging in a regulatory sense.

The New Zealand Law Commission identified that anonymous communications on the Internet raised issues for complainants because:

- the complainant cannot approach the communicator directly to seek redress
- the complainant may experience particular distress in not knowing where the communications originate from, and
- the extremity of the communication may be intensified under the cloak of anonymity.[105]

6.5 Issues with law enforcement

The existence of confidentiality agreements between service providers (such as Twitter and Facebook) and users, as well as the potential application of information privacy laws, can hinder the ability of people to access informal solutions in situations where other users have potentially infringed their rights in some way. The New Zealand Law Commission found that while 'the existing criminal and civil law could deal with many types of harmful digital communications', problems arise where people are required to initiate formal court proceedings in order to compel disclosure. These problems include:

- legal processes not operating within 'internet time' when information is disseminated virally and globally within minutes
- the cost of civil proceedings and restrictions on legal aid place access to the civil jurisdiction of the courts beyond the reach of many ordinary citizens – and 'given the evidential and legal complexities that surround litigation of 'online' matters, self-represented litigants face a daunting task'
- difficulties in bringing a criminal prosecution, primarily because the evidence gathering process can be complex and multi-jurisdictional, and police investigative resources are limited.[106]

A further obstacle to the effective enforcement of laws in relation to behaviour on the Internet is the cross-jurisdictional nature of online 'publication'. It may be difficult to predict how an Australian court order would or could be enforced on a company or individual based overseas but whose Internet service or site is accessed in Australia.

Given the number of major Internet service providers based in the United States, it is instructive to consider the Yahoo! case in 2000,[107] in which the Paris Superior Court rejected the argument that Yahoo! was protected by the First Amendment because it operated out of the US. The French court relied for jurisdiction on the fact that the effects were felt in France, and accordingly ordered Yahoo! to take all measures to prevent French citizens from accessing auction services for Nazi paraphernalia. Yahoo! were given three months to comply with the order or face a penalty of

100,000 Francs (US$13,300) for every day of non-compliance. Yahoo! subsequently won a motion in the United States District Court, with that Court declaring that the French court's order could not be enforced as it would contravene the First Amendment of the US Constitution.[108]

The Yahoo! case raises serious doubt about whether Australian court orders regarding behaviour in cyberspace which would involve multiple jurisdictions could be effectively enforced within a country like the United States.

For a discussion of some regional and international initiatives designed to try and address obstacles to the effective enforcement of laws targeting cross-jurisdictional criminal activity over the Internet, see section 7.3 below.

7 Are current regulatory responses sufficient and appropriate?

7.1 Federal anti-discrimination laws

Current federal anti-discrimination laws would generally apply to cyberspace to the extent that discriminatory behaviour (or harassment) online relates to a protected attribute, and could be said to have occurred in one of the stipulated areas of 'public' life. This is particularly clear in relation to the prohibition on sexual harassment under the *Sex Discrimination Act 1984* (Cth) (SDA), as this Act was amended in 2011 to ensure that online sexual harassment was captured.[109] So, for example, if someone is 'cyber -sexually harassed' at work by a colleague who is using a work computer (or work mobile phone), there would be a strong argument that this situation would be covered by the SDA. Concepts such as the 'workplace' and an 'education institution' have been interpreted to include sufficiently closely related 'cyberspace' within their boundaries.

However, within these defined areas of public life, a number of exceptions exist in terms of potential coverage. Further, the areas of public life currently covered by anti-discrimination laws will not necessarily extend to cover purely 'social' or 'informational' contexts. Online socialising through social network sites may be at once both a private and a public activity but is unlikely to fall within the ambit of, for example, employment, the provision of goods and services, accommodation or education. Yet despite this, many forms of cyber-discrimination and harassment have occurred and continue to occur on social networking and/or social media sites.

In contrast, the provisions of the federal RDA could potentially apply to these contexts. Unlike the SDA, the *Disability Discrimination Act 1992* (Cth) and the *Age Discrimination Act 2004* (Cth), the RDA is not limited to specified areas of public life. Rather, the general discrimination protections simply require that the act had the 'purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of any human right or fundamental freedom in the political, economic, social, cultural or **any other field of public life'**.[110] Similarly, the racial hatred provisions contained in the RDA apply to acts done 'otherwise than in private'.[111]

This broader construction of 'public life' under the RDA means that race discriminatory actions on online socialising or informational/social media platforms could be covered by the Act. For example, under the racial hatred provisions, the

placing of anti-Semitic material on a website which was not password protected was held by the Federal Court to be an act 'not done in private', and therefore subject to the protections of the RDA. [112] Accordingly, To the extent 'cyber-trolls' and others engage in cyber-racist behaviour on social networking and media sites, their actions could be covered by the provisions contained in the RDA.

There are limitations to the protection under the RDA, such as those in s 18D (which excludes from s 18C things done 'reasonably and in good faith' in the context of artistic works, discussions and debates, fair and accurate reporting and fair comment expressing a genuine belief).[113] One important limitation of the coverage of the RDA is the ability to actually enforce orders against hosts of such information. The RDA has an 'ancillary liability' provision which makes it unlawful to 'assist or promote' unlawful acts of discrimination, [114] which could capture the actions of 'hosts' (as opposed to the creator of the information).[115] However ancillary liability provisions do not apply to the racial hatred provisions.[116]

The need then to pursue the individual responsible for actually posting the offensive material creates significant difficulties where sites allow people to create and post information on websites or blog/socially network anonymously or pseudo-anonymously using multiple personae (issues of anonymity are discussed in detail above). [117] For example, it has been reported that in 2012 Facebook was ordered by the UK High Court to provide the email and IP addresses of a number of so-called 'cyber-bullies' so that a complainant could proceed with a private prosecution.[118]

While Facebook may informally agree to comply with orders such as these, formal enforcement of such orders in an overseas jurisdiction remains problematic (issues of multiple jurisdictions have been discussed above). The Commission faces similar difficulties in compelling disclosure of such information when trying to resolve complaints. Website hosts and social networking sites have informally complied with requests by the Commission to remove information. Yet despite the Commission having the power to compel disclosure of such information, this cannot actually be enforced without the overseas counterpart jurisdiction ordering such enforcement in compliance with its own jurisprudence (of which there is no guarantee).

7.2 Regulation of 'offensive' behaviour

(a) Overview

Where 'offensive' and/or bullying behaviour occurs that falls outside of a defined area of public life and does not attach to a protected attribute for the purposes of anti-discrimination laws, other laws may apply.

At the domestic level, the regulation of cyber-bulling and other forms of offensive behaviour are regulated by a complex array of federal and state laws. Federal and state workplace bullying health and safety regulations cover forms of cyber-bullying to the extent that they occur within the workplace. In terms of the regulation of offensive Internet behaviour more generally, the focus of federal laws is on regulating the conduct of Internet service providers or 'content hosts' of potentially offensive material.[119]

A somewhat anachronistic addition to this is a broad-ranging provision in the federal criminal law which prohibits the use of a carriage service in a manner which a reasonable person would find offensive.[120] In contrast to the federal focus on regulating 'content hosts', State and Territory laws impose obligations on producers of content.[121] A number of non-legislative initiatives also exist focusing on monitoring and educating the public about content on the Internet. These forms of regulation are described in further detail below.

(b) Regulation of workplace (cyber)bullying

Cyber-bullying has brought the issue of the regulation of 'offensive behaviour ' on the Internet to the forefront of government, media and community attention. As discussed above, the issue of cyber-bullying clearly engages a number of human rights recognised under international law. In Australia, bullying which is not covered by anti-discrimination laws may be covered by work health and safety legislation, by criminal laws in Victoria and by the Commonwealth *Criminal Code Act 1995*. Uniform work health and safety legislation has been adopted by the Commonwealth, four States and the Territories since 2011.

The *Work Health and Safety Codes of Practice 2011: How to manage work health and safety risks*[122] operates under the *Work Health and Safety Act 2011* and applies to all bodies and persons having duties under the Act. The Code includes bullying in the definition of hazard, and describes workplace bullying as a work-related health issue.[123] The effect of this is that employers and officers have a duty to prevent workplace bullying, and workers and other people at the workplace have a duty not to engage in workplace bullying. Similarly, in Victoria and Western Australia (jurisdictions which have not adopted the uniform legislation) 'bullying' has been interpreted as included in concepts of 'health and safety risk'[124] and 'hazard'.[125] There appears to be nothing in workplace bullying provisions to preclude coverage of workplace 'cyber-bullying'.

As for the provisions contained in Victorian[126] and Commonwealth[127] criminal law, these are not limited to the workplace and cover behaviours that constitute 'cyber-bullying'. These provisions are covered in further detail below.

(c) Regulation of Internet providers and content hosts

At the federal level, apart from the workplace-specific bullying regulations described above, the focus of the regulation of offensive behaviour centres on those who **host** offensive content on the Internet (as opposed to those who create it). The *Broadcasting Services Act 1992* (Cth) aims to restrict access to or prohibit certain types of offensive Internet content, and provides a complaints mechanism.[128] It prohibits Internet content that is (or would be) classified as 'Refused Classification' (RC) which applies to publications, films or computer games that:

- depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena, in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be accorded a classification other than RC; or

- describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not); or
- promote, incite or instruct in matters of crime or violence.[129]

These provisions apply to very serious forms of 'offensive' content which may include extreme forms of cyber-bullying. This scheme does not target, for example, 'hate speech'. As a result, this scheme does not represent an avenue of redress against a person or group who is vilified by Internet hate speech in Australia. However, in extreme cases where online content incites crime or violence (which could, for example be racially based), the Australian Media and Communications Authority (ACMA) could issue a removal notice.[130]

ACMA investigates complaints about online content that may be 'prohibited content' according to criteria of the National Classification Code (set out above). Where the content is classified as 'prohibited', ACMA issues a series of notices to Australian-based hosts requiring either the removal of the content, or restricted access within a set timeframe (failing which a penalty applies). Where Australian-hosted prohibited content is considered to be sufficiently serious, ACMA must notify law enforcement agencies.[131] Apart from providing filtering software options, where sufficiently serious prohibited content is hosted outside Australia, ACMA notifies a 'member hotline' in the country where the content appears to be hosted or in the absence of a hotline, notifies the Australian Federal Police for action through Interpol.[132]

A co-regulatory framework based on industry codes also forms part of the scheme under the *Broadcasting Services Act 1992* (Cth).[133] These codes may be developed by the industry,[134] or required by ACMA,[135] and are registered and enforced by ACMA.[136] Two industry codes that have been developed impose various obligations on content hosts, ISPs, mobile carriers, and content service providers, including:

- obligations in responding to notices
- requirements about what information must be provided to users
- requirements about making filters available
- requirements about establishing complaints procedures and
- the appropriate use of restricted access systems.[137]

There are, however, significant regulatory challenges in attempting to enforce classification laws in relation to online media content, including:

- inconsistency in offence and penalty provisions between Australian jurisdictions;[138]
- the quantity and mutable nature of online content;
- the number of persons producing content and its hosting all over the world; and
- the difficulty of determining age and of restricting content.[139]

(d) Regulation of producers of content and upload of/access to content

Certain state and territory laws contain provisions directly regulating the actual production and use (as opposed to hosting) of online content. For example, the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic) makes it an offence to 'use an on-line information service to publish or transmit, or make available for transmission' objectionable material, child pornography or 'material unsuitable for minors'.[140]

In addition to these provisions, all Australian jurisdictions have laws dealing with cyber-stalking – a behaviour that can form part of 'cyber-bullying'. A number of states have explicitly extended the definition of this crime to include the sending of electronic messages.[141] At the Commonwealth level offences relating to behaviour on the Internet[142] includes cyber-fraud and stalking;[143] threats to kill or cause serious harm;[144] making hoax threats;[145] and most relevantly, engaging in conduct that a *reasonable person* would find to be menacing, harassing or cause offence.[146]

It is instructive to consider that similar legislative provisions in the UK have been used to prosecute individuals for various forms of 'offensive behaviour' in cyberspace.[147] This includes situations where a teenager made offensive comments about a murdered child on Twitter; a young man wrote on Facebook that British soldiers should 'go to hell' and a third posted a picture of a burning paper poppy (a symbol of remembrance of war dead).[148] According to news reports all were arrested, two were convicted, and one jailed.[149]

Concerns about the impact of these prosecutions on freedom of expression led the UK Director of Public Prosecutions to release guidelines on prosecuting cases involving social media communications, in recognition that an excess of prosecutions 'chills' free speech and that a higher threshold for prosecution was required.[150] The interim guidelines are intended to 'strike the right balance between freedom of expression and the need to uphold criminal law'.[151]

The guidelines state that if someone posts a message online that clearly amounts to a credible threat of violence, specifically targets an individual or individuals, or breaches a court order designed to protect someone, then the person behind the message may be prosecuted.[152] People who receive malicious messages and pass them on (i.e. by re-tweeting) can also be prosecuted.[153] However, the guidelines provide that online posts that are merely 'grossly offensive, indecent, obscene or false' must reach a higher threshold before the conduct would be considered for prosecution, and in many such cases a prosecution is unlikely to be in the public interest.[154]

In Australia, other offences aimed particularly at the protection of children on the Internet include laws criminalising sexual grooming (targeting the use of a carriage service, the Internet or mobile phone for sexual activity with children),[155] and using a carriage service to send or receive child pornography (which may capture some 'sexting').[156] Distributing images can be a form of cyber-bullying if a young person is coerced into posing, or if images are distributed without consent.[157] Further, in 2011 the SDA was amended in 2011 to give legal protection to young people who have experienced sexual harassment (including online) at an educational institution by permitting students under the age of 16 to lodge a complaint under that Act.[158]

Criminal offences also exist against the promotion of suicide on the Internet.[159]

7.3 International (cross-jurisdictional) regulatory initiatives

An example of a regional approach to regulating racist hate speech on the Internet is the European *Additional Protocol to the Convention on Cybercrime*.[160] The aim of the Additional Protocol is to limit or at least reduce the amount of hate material online by requiring States Parties to criminalise the 'making available' or 'distribution' of racist or xenophobic material through a computer system within their jurisdictions. The Protocol creates a legal framework for international co-operation in the prosecution (at the domestic level) of cross-jurisdictional hate speech in cyberspace.[161]

The Australian Government has ratified the *European Convention on Cybercrime*,[162] which focuses on international cooperation to combat cybercrime.[163] However it has not signed or ratified the Additional Protocol dealing with racist hate speech online.

At the international level, non-mandatory principles in relation to conduct on the Internet have been proposed for domestic adoption.

In 2001 the Durban Declaration and Plan of Action was adopted at the United Nations World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance. The Durban Declaration contains principles relating to racism on the Internet which recognise both the capacity of the Internet as a tool to promote tolerance and educate others, and the need to avoid use of the Internet which promotes racism and intolerance.[164] The Plan of Action includes calling on States to impose legal sanctions in respect of incitement to racial hatred through new information and communications technologies, including through the Internet.[165]

In 2003 at the United Nations World Summit on the Information Society a *Plan of Action* was produced, which stated that:

> All actors in the Information Society should take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs [Information and Communication Technologies], such as illegal and other acts motivated by racism, racial discrimination, xenophobia and related intolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings.[166]

The idea for an International Criminal Court or Tribunal for Cyberspace has also been raised by a number of advocates.[167] However the draft proposal is limited to the 'most serious violations of international cybercrime law' and may not capture or resolve all the issues raised here.[168]

7.4 Non-legislative initiatives

Alongside formal 'legislative measures', a number of 'non-legislative' measures are being utilised in regulating offensive forms of online behaviour. Importantly, a number of these measures are aimed at preventative behaviour-change (as opposed to reactive legislative responses). Such measures include the development of company policies; co-regulatory measures (between industry and a regulator(s)); voluntary codes of practice and general educative/attitudinal change initiatives.

In Australia, examples of such measures include:

- Self-regulation by websites through the adoption of codes of conduct (see, for example, Facebook's 'Statement of Rights and Responsibilities').[169] This includes 'unofficial' regulation by internet service providers/content hosts in responding to informal requests to remove material.
- The 'Cybersmart' education program created by the Australian Government and ACMA.[170] This program is designed to providing information and education to children and young people to empower them to be safe online, and to support parents, teachers and library staff. It aims to build resilience through cyber-smart behaviour and an awareness of rights and consequences.
- The Australian Government's Cybersafety Help Button initiative,[171] which provides users (particularly children and young people but also parents/carers and teachers) with easy online access to a wide range of cyber-safety and security resources to help with cyber-bullying, unwanted contacts, scams, frauds and inappropriate material.
- *Back me up,*[172] a social media campaign run by the Commission to encourage young people to take positive action to support friends or peers who are cyber-bullied. It offers young people information about how to take safe and effective action when they witness cyber-bullying.
- The *Consultative Working Group on Cyber-safety* (in which the Commission participates).[173] The Group considers those aspects of cyber safety that particularly affect Australian children, such as cyber bullying, identity theft and exposure to illegal and inappropriate content. It provides advice to the Australian Government on priorities and measures needed to ensure world's best practice safeguards for Australian children engaging in the digital economy.

7.5 Other proposals for responding to discrimination, harassment and hate speech online

(a) Legislative reform

A number of legislative reforms have been proposed in relation to the regulation of the issues discussed above in section 5 of this paper.

For example, in relation to the cyber-safety of young people, the Parliamentary Joint Select Committee on Cyber-Safety has identified privacy laws as an area in need of 'cyber-reform'.[174] The reforms suggested by the Committee included:

- amending the small business exemption where these businesses transfer personal information offshore;[175]
- developing guidelines on the appropriate use of privacy consent forms for online services;[176]
- imposing a code which includes a 'Do Not Track' model;[177]
- ensuring privacy laws cover organisations that collect information from Australia[178]

- reviewing the enforceability of provisions relating to the offshore transfer of data.[179]

In addition, the Joint Select Committee recommended that training be provided to all Australian Police Forces as well as judicial officers to ensure they are adequately equipped to address cyber-safety issues.[180] It also recommended that a National Working Group on Cybercrime be created to undertake a review of legislation in Australian jurisdictions relating to cyber-safety crimes.[181] The report also explored the proposal of creating an online Ombudsman to deal with cyber-safety issues.[182]

It is interesting to note that the New Zealand Law Commission recommended a number of legislative reforms in that jurisdiction in respect of 'harmful digital communications'. This included the creation of a new communications offence targeting all types of digital communications (including through social media) which are 'grossly offensive or of an indecent, obscene or menacing character' **and** which cause harm.[183] It also recommended making it an offence to publish intimate photographs or recordings of another person without their consent,[184] and to incite a person to commit suicide, irrespective of whether or not the person does so.[185]

It further proposed the establishment of a specialist Communications Tribunal capable of providing speedy, cheap and efficient relief outside the traditional court system.[186] This Tribunal would in effect operate as a mini-harassment court specialising in digital communications (using mediation to resolve trivial matters),[187] and providing civil remedies such as takedown orders and cease and desist orders.[188] The New Zealand Law Commission proposed that it would be the option of last resort, and that the threshold for obtaining a remedy would be high.[189]

(b) Other measures

Over the next 3 years the Commission will be partnering with academia as part of an Australian Research Council project on cyber-racism and community resilience. The project will include a review of the Australian legal, regulatory and policy framework that surrounds racist speech on the Internet. The aim of the project is to contribute towards the development of new approaches to the regulation of cyber-racism and to co-operative work between industry and regulators to improve responses to cyber-racism.

The Joint Select Committee on Cyber-Safety in its report on Cyber-safety and young people proposed various educative measures, including:

- development of an agreed national definition of cyber-bullying[190]
- introduction of a cyber-safety student mentoring program[191]
- national core standards for cyber-safety education in schools[192]
- a national online training program for teachers and students that addresses bullying and cyber-bullying[193]
- the introduction nationally of 'Acceptable Use' agreements governing access to the online environment by students[194] and the use of resources such as the CyberSafety Help Button[195]

- the incorporation of cyber-safety materials into teacher training courses,[196] including advice about available processes in the event of cyber-bullying[197]
- the promotion of self-assessment tools,[198] and investigation of the information made available to parents at 'point of sale' of computers and mobile phones.[199]
- increasing affordable access to crisis help lines[200]
- enhancing the effectiveness of cyber-safety media and educational campaigns[201] including making materials available through a central portal.[202]

The Joint Select Committee also proposed industry-based initiatives, including that the Australian Government encourage the Internet Industry Association to increase accessibility to assistance and complaints mechanisms on social networking sites,[203] and negotiate protocols with overseas networking sites to ensure the timely removal of offensive material.[204]

The non-legislative recommendations of the New Zealand Law Commission included:

- requiring all schools to implement effective anti-bullying programs[205]
- establishing on-going data collection (including measurable objectives and performance indicators) for defining and measuring covert and overt forms of bullying[206] and developing reporting procedures and guidelines[207]
- consideration of the use of Information and Technology contracts which are routinely used in schools, to educate students about their legal rights and responsibilities with respect to communication[208]
- the development of consistent, transparent and accessible policies and protocols for how intermediaries and content hosts interface with domestic enforcement mechanisms.[209]

8 A right to access the Internet

While there appears to be no express right of general application to 'access cyberspace/the Internet' stipulated in any of the major international human rights instruments, [210] it has been argued at the international level that such access is critical, particularly in terms of the right to freedom of expression, and in the redressing of structural disadvantage. Accordingly a number of countries have, in varying forms, formally recognised human rights to access the Internet. These trends are considered below, along with developments within the Australian context.

8.1 At the international level

The Special Rapporteur argues that without Internet access 'which facilitates economic development and the enjoyment of a range of human rights, marginalized groups and developing States remain trapped in a disadvantaged situation'.[211] This has been characterized as the 'digital divide', being 'the gap between people with effective access to digital and information technologies, in particular the Internet, and those with very limited or no access at all'.[212] The Special Rapporteur asserts the positive obligation on States to 'promote or to facilitate the enjoyment of the right to

freedom of expression and the means necessary to exercise this right, including the Internet' as a means of overcoming this divide.[213]

According to the Special Rapporteur, access to the Internet is seen as critical to combating situations of inequality, by ensuring that marginalized or disadvantaged sections of society can express their grievances effectively and that their voices are heard.[214] He argues that the Internet 'offers a key means by which such groups can obtain information, assert their rights, and participate in public debates concerning social, economic and political changes to improve their situation'.[215] It also offers an important educational tool in making accessible previously unaffordable academic material to people in developing countries.[216]

However, the Special Rapporteur acknowledges that disadvantaged groups 'often face barriers to accessing the Internet in a way that is meaningful, relevant and useful to them in their daily lives'.[217]

One academic, Cees Hamelink, argues that if the right to freedom of expression is interpreted in more than the classical negative sense (that is, as a 'positive right' and not merely as a liberty), it becomes a 'claim-right'.[218] This means a person not only has the right to express opinions, but also, by implication, to the related entitlement to facilities for the exercise of this right. The recognition of freedom of expression as a positive claim-right is particularly important in situations where the voices of some people are systematically excluded.[219]

Mr Hamelink further argues that human rights in cyberspace should not only be articulated as individual rights, but also recognised as collective rights.[220] A collective right of access to the Internet for communities, he postulates, is critical given that there are certain groups of people who tend to be excluded from full access to the Internet (he mentions women, ethnic minorities and lower socio-economic groups). He argues that collective claims can also include the right to development (of communication infrastructures), and a right to the sharing of knowledge and skills resources.[221]

The recommendations of the United Nations 2003 World Summit on the Information Society reflect the need for specific attention to be given to vulnerable groups. The *Plan of Action* adopted at that Summit included that States 'promote research and development to facilitate accessibility of ICTs for all, including disadvantaged, marginalized and vulnerable groups.'[222] It was proposed that:

> national e-strategies address the special requirements of older people, persons with disabilities, children, especially marginalized children and other disadvantaged and vulnerable groups, including by appropriate educational administrative and legislative measures to ensure their full inclusion in the Information Society.[223]

'Full inclusion' would extend beyond mere access rights, and would include initiatives to build confidence and security in the use of the Internet. In practice, this could include Governments establishing 'sustainable multi-purpose community public access points' and providing affordable or free Internet access to their citizens.[224]

Practical developments at the international level in respect of the 'right to access the Internet' include, as part of the Millennium Development Goals, a formal target calling upon States 'in consultation with the private sector [to] make available the benefits of

new technologies, especially information and communications'.[225] Other initiatives include: [226]

- the 'One Laptop Per Child' project (supported by the United Nations Development Programme), which aims to spread the availability of the Internet into developing countries (currently this is being progressively implemented in countries such as Uganda and Rwanda)
- the Indian Government's 'public-kiosks' program
- the Brazilian government's 'computers for all' program offering subsidies for the purchasing of computers.

The Special Rapporteur has reported that Internet access has been expressly recognized as a human right in some economically developed States:

> For example, the parliament of Estonia passed legislation in 2000 declaring Internet access a basic human right.52 The constitutional council of France effectively declared Internet access a fundamental right in 2009, and the constitutional court of Costa Rica reached a similar decision in 2010.53 Going a step further, Finland passed a decree in 2009 stating that every Internet connection needs to have a speed of at least one Megabit per second (broadband level). [227]

8.2 At the domestic level

Within the Australian context, the Commission has developed World Wide Web Access Advisory notes which provide guidance on the requirements for compliance with the *Disability Discrimination Act 1992* (Cth)[228] The Advisory notes provide important practical information on how to make websites more accessible to people with a disability who, like the rest of the community, rely increasingly on the Internet to access a wide range of often critical information and service provision. The notes also provide information about how web designers and website owners can minimise the possibility of disability discrimination.

The Commission has also considered the right to Internet access in the context of older people in its submission to the Joint Select Committee Inquiry into Cybersafety for Senior Australians.[229] The Commission submitted that 'due to the speed with which the information technology revolution has occurred, many older people in Australia had found themselves on the wrong side of the digital divide'.[230]

Internet access to essential services and social networking potentially provides older people with the option to live autonomously in their homes for longer. Yet many older people, particularly those aged 65 and above, missed the information technology agenda that is now part of mainstream education, resulting in a lack of confidence to engage with the Internet at a high level. This can preclude their 'full inclusion' in accessing mainstream information technology and in making independent decisions about their lives. The social and economic consequences of the relative disadvantage experienced by older Australians in using the Internet has led Age Discrimination Commissioner Susan Ryan to characterize this disadvantage as a form of age discrimination.[231]

Evidence from the Australian Institute of Criminology (AIC) indicates that older people in Australia have difficulties managing their online security, and that people

over the age of 65 are more likely to be victims of online financial fraud than any other age group.[232] The Australian Crime Commission has highlighted that organised criminal networks take advantage of new technologies to expand their reach, commit crimes from a distance, create the appearance of legitimacy and exploit the lack of clear jurisdictional authority.[233] This in turn increases the threat and harm caused to the Australian community, particularly to older people who might be more specifically targeted.[234]

As mentioned above, the Australian Government has ratified the *European Convention on Cybercrime*. Prior to ratifying the Convention, the Australian Government enacted the *Cybercrime Legislation Amendment Act 2012* (Cth) (the Cybercrime Act), to ensure that Australian legislation meet all the requirements under the Convention (subject to certain reservations).[235] The main objective of the Convention (and therefore the Cybercrime Act) is to pursue a common criminal policy aimed at the protection of society against cyber-crime, especially by adopting appropriate legislation and fostering international co-operation.[236]

While the passage of the Cybercrime Act and Australia's ratification of the Convention is an important step, it represents a largely reactive approach. To be truly effective, a preventative approach must also be undertaken of educating users on 'cyber-safe' practices when engaging with information technology. However, evidence suggests that despite some success, current Internet training arrangements for older people require more targeted initiatives to engage segments of the aged population who do not respond to current programs and schemes.

These issues of access, confidence and security do not just affect older people in Australia and people with disability,[237] but can impact on people from culturally and linguistically diverse backgrounds, remote communities where ICT infrastructure is most deficient, and people from lower socio-economic backgrounds who cannot always individually afford access to these technologies.

In order to ensure that information is truly accessible to all people in Australia, government departments and/or private companies should audit online materials to ensure they are user-friendly for new Internet users; institute educative initiatives on the secure use of the Internet and increase opportunities for meaningful access to the Internet of marginalised groups. Only when these measures are in place can structural vulnerability be identified, 'full inclusion' be achieved and any notion of the 'right' to access the Internet be truly realised.

9 Conclusion

It is clear that the Internet provides unparalleled opportunities for the promotion and advancement of human rights, most centrally the right to seek, receive and impart information. The Special Rapporteur on that right has described the Internet as 'one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies.'[238] He has accordingly stated that 'facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States.'[239]

However, the Internet also provides a new (and powerful) medium through which persons can (and do) publish hateful or discriminatory comments, and intimidate and harass others, in a manner which undermines the human rights of those who are targeted.

Accordingly, societies' use of the Internet raises challenging questions about the appropriate balancing of rights in cyberspace. Difficult questions of how to simultaneously protect potentially competing rights are not unique to the online environment. But the particular features of the Internet (its global (and therefore cross-jurisdictional) and instant reach; its creation of an effectively permanent record of communications, and the ability to communicate anonymously) present new obstacles for governments seeking to protect against harmful behaviour.

These types of issues must be addressed in order for Australia to fulfil the theoretically simple (but practically very challenging) requirement that 'the same rights that people have offline must also be protected online'.[240]

10 Questions for discussion

There are two broad challenges regarding human rights and use of the Internet which emerge from the discussion in this paper, namely:

1. How do we as a society achieve an appropriate balance between competing rights in an online environment?
2. What steps should be taken to address discrimination in terms of the ability of certain groups to access (and safely utilise) the Internet?

10.1 Addressing discrimination in terms of access to (and use of) the Internet

The growing importance of the Internet to all aspects of life (including delivery of services by business and government) means that the 'digital divide' between those with effective access to the Internet and those without limits the latter group's ability to enjoy a range of human rights. In order to effectively address this gap in enjoyment of rights (particularly the right to freedom of expression and information), consideration should be given to the following:

(a) What groups in Australia are affected by the 'digital divide'?

(b) To what extent does this impact on their enjoyment of rights?

(c) What measures should be taken to address the difficulties that the following groups may experience in accessing the Internet:

  (i) people with disability

  (ii) older Australians

  (iii) Indigenous Australians

  (iv) Australians living in remote or rural areas?

(d) To what extent would the 'digital divide' be addressed by ensuring access for all Australians to Internet facilities? How relevant are issues such as digital literacy and cyber-crime to the effective enjoyment of rights through the Internet for these groups?

10.2 Balancing rights online

A key challenge in terms of ensuring that individuals' rights are protected online is achieving an appropriate balance between protecting the right to freedom of opinion and expression in cyberspace, and protecting people from online bullying, discrimination and harassment which breaches their rights under the ICCPR. The types of issues which need to be explored include:

(a) How prevalent is online hate speech (i.e. racial vilification, hate speech against women, LGBTI people) - is it only a small minority who posts this extreme content, or is there a wider problem?

(b) Are online hate speech, discrimination and verbal abuse different to hate speech, discrimination and verbal abuse that occur in the offline world - does the potential reach and permanency of internet content change the impacts of these types of behaviours?

(c) Are (reactive) legislative measures, rendering behaviour unlawful or criminal, an appropriate (and/or effective) way of achieving a balance between the competing rights in an online environment?

(d) For the purposes of the application of anti-discrimination laws, what should be considered a 'public' vs. a 'private' space in the online world?

(e) To what extent are (preventative) educative measures an effective way of addressing online hate speech and discrimination?

(f) What type of laws, polices and/or practices do we need to create safe online environments for children, to ensure that they enjoy their rights in cyberspace (including the right to freedom of expression and to information)?

11 Further information

As mentioned above, the Commission has worked and continues to work on a range of human rights issues connected with the Internet. Further information can be found on the Commission's webpage 'Human rights and the Internet', at http://www.humanrights.gov.au/human-rights-and-internet. This includes links to the Commission's work relating to:

- access and accessibility for people with disability
- access and online safety for older Australians
- racial discrimination and vilification in online environments
- sexual harassment over the Internet
- cyber safety for children and cyber-bullying
- online safety in Indigenous communities.

[1] See D Connolly, *A little history of the World Wide Web*, http://www.w3.org/History.html (viewed 27 August 2013).
[2] International Telecommunication Union, Key 2006-2013 ICT data for the world, by geographic regions and by level of development, for the following indicators, at *http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/ITU_Key_2005-2013_ICT_data.xls* (viewed 27 August 2013).
[3] Opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976) (ICCPR), art 9(1), at http://www.austlii.edu.au/au/other/dfat/treaties/1980/23.html (viewed 27 August 2013).
[4] Human Rights Committee, *General Comment No. 34 – Article 19: Freedoms of opinion and expression,* UN Doc CCPR/C/GC/34 (2011). At http://tbinternet.ohchr.org/_layouts/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11 (viewed 27 August 2013).
[5] Human Rights Committee, *General Comment No. 34*, note 4, para 12.
[6] See the Commission's page on permissible limitations on human rights at http://www.humanrights.gov.au/permissible-limitations-rights.
[7] *The promotion, protection and enjoyment of human rights on the Internet*, Human Rights Council Resolution 20/8, UN Doc A/HRC/RES/20/8 (2012), para 1. At http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8 (viewed 27 August 2013).
[8] At http://www.humanrights.gov.au/human-rights-and-internet.
[9] F La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Report to the Human Rights Council, 17th session, UN Doc A/HRC/17/27 (2011), p 7. At http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx (viewed 27 August 2013.
[10] F La Rue, above, p 7.
[11] F La Rue, above, p 19.
[12] F La Rue, above.
[13] D Rolph, M Vittins and J Bannister, *Media Law: Cases, Materials and Commentary* (2010), pp 23-26.
[14] D Rolph, M Vittins and J Bannister, above, p 23.
[15] Human Rights Committee, *General Comment No. 34*, note 4, para 13.
[16] D Rolph, M Vittins and J Bannister, note 13, p 23.
[17] Human Rights Committee, *General Comment No. 34*, note 4, para 11 (emphasis added).
[18] F La Rue, note 9, p 7.
[19] See the *Human Rights Act 2004* (ACT) and *Charter of Human Rights and Responsibilities Act 2006* (Vic).
[20] See the Commission's page *Common law rights and human rights scrutiny* for more discussion: http://www.humanrights.gov.au/common-law-rights-and-human-rights-scrutiny.
[21] See *Brown v Classification Review Board* (1997) 154 ALR 67, in which French J stated (at 76): 'A person may say and write anything he pleases except in so far as he may not'. See also *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, in which the High Court stated (at 567): 'Within our legal system, communications are free only to the extent that they are left unburdened by the laws that comply with the Constitution'.
[22] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 599. See *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1; *Australian Capital Television Pty Ltd & New South Wales v Commonwealth* (1992) 177 CLR 106, and the discussion in D Rolph, M Vittins, J Bannister, note 12, pp 32-43.
[23] See the 'urging violence' offences in ss 80.2 – 80.2B of the *Criminal Code Act 1995* (Cth).
[24] See, for example, the restrictions which may be placed on communication by certain individuals who are made the subject of control orders or preventative detention orders: *Criminal Code Act 1995* (Cth) s 104.5(3)(e) and ss 105.15, 105.16, and 105.34.
[25] See the offences in Part 10.6, Div 474, Sub-div C of the *Criminal Code Act 1995* (Cth).
[26] See, for example, *Racial Discrimination Act 1975* (Cth) s 18C; *Anti-Discrimination Act 1977* (NSW) s 20C; *Racial and Religious Tolerance Act 2001* (Vic) ss 7 and 8.
[27] See the *Copyright Act 1968* (Cth).
[28] See the discussion in N O'Neill, S Rice and R Douglas, *Retreat From Injustice: Human Rights Law in Australia* (2nd ed, 2004), Chapter 17.
[29] See, for example, *Crimes Act 1900* (NSW) s 327.

[30] See the discussion in N O'Neill, S Rice and R Douglas, note 28, Chapter 16, particularly the section entitled 'Contempt by Criticising or "Scandalising" the Courts'.
[31] See, for example, *Crimes Act 1900* (NSW) s 192G.
[32] See the *Privacy Act 1988* (Cth).
[33] See for example *Classification (Publications, Films and Computer Games) Act 1995* (Cth) and the *Broadcasting Services Act 1992* (Cth).
[34] F La Rue, note 9, p 9.
[35] A Moses, 'Filter was white elephant waiting to happen', *The Sydney Morning Herald*, 9 November 2012. At http://www.smh.com.au/technology/technology-news/filter-was-white-elephant-waiting-to-happen-20121109-2923o.html (viewed 27 August 2013).
[36] F La Rue, note 9, p 10.
[37] F La Rue, above.
[38] See http://www.humanrights.gov.au/right-freedom-information-opinion-and-expression#other.
[39] Opened for signature 20 November 1989, 1577 UNTS 3 (entered into force 2 September 1990) (CRC). At http://www.austlii.edu.au/au/other/dfat/treaties/1991/4.html (viewed 27 August 2013).
[40] Opened for signature 30 March 2007, 2515 UNTS 3 (entered into force 3 May 2008). At http://www.austlii.edu.au/au/other/dfat/treaties/ATS/2008/12.html (viewed 27 August 2013).
[41] *Universal Declaration of Human Rights*, UN General Assembly Resolution 217A(III), UN Doc A/810, 71 (UDHR) (1948). At http://www.un.org/en/documents/udhr/ (viewed 27 August 2013).
[42] Human Rights Committee, *General Comment No. 34*, note 4, para 21.
[43] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Examination of legislation in accordance with the* Human Rights (Parliamentary Scrutiny) Act 2011*: Bills introduced 12 – 14 March 2013,* Fourth report of 2013 (2013), para 1.69. At http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=humanrights_ctte/reports/index.htm (viewed 27 August 2013).
[44] Human Rights Committee, *General Comment No. 34*, note 4, para 22.
[45] Human Rights Committee, *General Comment No. 34*, note 4, para 25.
[46] The permissible grounds for restrictions listed in article 19(3) include restrictions on the grounds of public health or national security, but discussion of circumstances in which these grounds might justify a limitation on the right to freedom of expression and to information as exercised through the Internet falls outside the scope of this present paper.
[47] Opened for signature 19 December 1966, 993 UNTS 3 (entered into force 3 January 1976) (ICESCR). At http://www.austlii.edu.au/au/other/dfat/treaties/1976/5.html (viewed 27 August 2013).
[48] Human Rights Committee, *General Comment No. 34*, note 4, para 50.
[49] Human Rights Committee, *General Comment No. 34*, note 4, para 48.
[50] See the Commission's Violence, Harassment and Bullying page: http://bullying.humanrights.gov.au/.
[51] Committee on the Rights of the Child, *General Comment No. 8 (2006) - The right of the child to protection from corporal punishment and other cruel or degrading forms of punishment*, UN Doc CRC/C/GC/8 (2006), para 11. At http://tb.ohchr.org/default.aspx?Symbol=CRC/C/GC/8 (viewed 27 August 2013).
[52] Human Rights Committee, *General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN Doc A/43/40 (1988), para 1. At http://www.refworld.org/docid/453883f922.html (viewed 27 August 2013).
[53] Human Rights Committee, *General Comment No. 16,* above, para 7.
[54] Human Rights Committee, *General Comment No. 34*, note 4, para 32.
[55] Human Rights and Equal Opportunity Commission, Letter to Ministers dated 9 May 1991 (Initial submission on proposed ban on political advertising) (1991), p 12 (citations omitted). At http://www.humanrights.gov.au/right-freedom-information-opinion-and-expression-0#Submissions
[56] See Human Rights Committee, *General Comment No. 34*, note 4, para 46.
[57] Human Rights Committee, *General Comment No. 34*, note 4, para 34.
[58] Human Rights Committee, *General Comment No. 34*, note 4, para 35.
[59] For a definition of an (Internet) meme see: http://netforbeginners.about.com/od/weirdwebculture/f/What-Is-an-Internet-Meme.htm (viewed 27 August 2013).

[60] This definition is drawn from definition used by the National Centre Against Bullying: see http://www.ncab.org.au/whatisbullying/ (viewed 28 August 2013). It should be noted that there are numerous and varying definitions of 'bullying'.
[61] Australian Communications and Media Authority, 'Australia in the digital economy, shift to the online environment', *Communications Report 2009-10 Series,* (June 2010), p 13.
[62] See the Alannah and Madeline Foundation's *Bullying Hurts* brochure at http://www.amf.org.au/FactSheets (viewed 28 August 2013).
[63] UDHR, art 25; ICESCR, art 12(1); CRC, art 24.
[64] UDHR, art 23; ICESCR arts 6 and 7.
[65] UDHR, art 19; ICCPR, art 19.
[66] CRC, art 31.
[67] The Committee also encouraged Australia to develop programs and strategies to use mobile technology, media advertisements and the internet to raise awareness among both children and parents on information and material injurious to the well-being of children: see Committee on the Rights of the Child*: Concluding Observation: Australia*, UN Doc CRC/C/15/Add.268 (20 October 2005) paras 33-34. At http://tb.ohchr.org/default.aspx?Symbol=CRC/C/15/Add.268 (viewed 28 August 2013).
[68] UDHR, art 26; ICESCR, art 13(1); CRC, art 29; Committee on the Rights of the Child, *General Comment No. 1 - Article 29 (1): The Aims of Education*, UN Doc CRC/GC/2001/1 (2001), para 8, at http://www2.ohchr.org/english/bodies/crc/comments.htm (viewed 28 August 2013).
[69] UDHR, art 5; ICCPR, art 7; CRC, art 19.
[70] A Moses and A Lowe, 'Contents removed form racist Facebook page", *The Sydney Morning Herald*, 8 August 2012, http://www.smh.com.au/technology/technology-news/contents-removed-from-racist-facebook--page-20120808-23tr1.html (viewed 27 August 2013).
[71] A Moses and A Lowe, above.
[72] A Moses and A Lowe, above.
[73] Australian Human Rights Commission, *Working without fear; Results of the Sexual Harassment National Telephone Survey* (2012) p 23. At http://www.humanrights.gov.au/working-without-fear-results-sexual-harassment-national-telephone-survey (viewed 27 August 2013).
[74] J Maley, 'The disturbing phenomenon of 'creep-shots'', *The Sydney Morning Herald*, 27 September 2012. At http://www.dailylife.com.au/news-and-views/dl-opinion/the-disturbing-phenomenon-of-creepshots-20120926-26kl5.html (viewed 27 August 2013).
[75] J Sinnerton and S Healy, 'Facebook 'sluts' page makers vow to return', *Herald Sun*, 13 October 2012. At http://www.heraldsun.com.au/news/james-silverwood-and-dom-terry-creators-of-banned-12-year-old-sluts-facebook-page-vow-to-return/story-e6frf7jo-1226494768239 (viewed 27 August 2013).
[76] J Sinnerton & S, Heal, above.
[77] L Hillier, P Horsely and C Kurdas, '"It made me feel braver, I was no longer alone": The Internet and same sex attracted young people' in J Nieto, *Sexuality in the Pacific* (2004), p 15.
[78] See the site 'No homophobes' at http://www.nohomophobes.com/#!/all-time/ (viewed 27 August 2013).
[79] See for example J Schwartz, 'Bullying, Suicide, Punishment', *The New York Times,* 2 October 2010. At www.nytimes.com/2010/10/03/weekinreview/03schwartz.html?_r=1&ref=tyler_clementi (viewed 27 August 2013).
[80] Times Topics, *'Tyler Clementi'*, *The New York Times*, 16 March 2012. At http://topics.nytimes.com/top/reference/timestopics/people/c/tyler_clementi/index.html (viewed 27 August 2013).
[81] New Zealand Law Commission, *Harmful Digital Communications: The adequacy of the current sanctions and remedies*, Ministerial Briefing Paper (August 2012), p 78. At http://www.lawcom.govt.nz/project/review-regulatory-gaps-and-new-media/publication/ministerial-briefing/2012/ministerial-briefing-harmful-digital-communications-adequacy-current-sanctions-and-remedies (viewed 28 August 2013).
[82] S Joseph, 'Free Speech, Racial Intolerance and the Right to Offend – Bolt before the court' (2011) 36(4) *Alternative Law Journal* 225, p 226.
[83] New Zealand Law Commission, note 81, p 27.
[84] New Zealand Law Commission, above, p10.
[85] New Zealand Law Commission, above, p 100.

[86] D Fogarty, 'Suppression order on Bayley background', *The Sydney Morning Herald*, 11 October 2012. At http://news.smh.com.au/breaking-news-national/suppression-order-on-bayley-background-20121011-27f3j.html (viewed 28 August 2013).
[87] *General Television Corporation Pty Ltd v DPP & Anor* [2008] VSCA 49, [70] (citations omitted).
[88] F La Rue, note 9, p 4.
[89] *The promotion, protection and enjoyment of human rights on the Internet,* note 7, para 2.
[90] F La Rue, note 9, p 8.
[91] New Zealand Law Commission, note 81, p 10.
[92] F La Rue, note 4, p 15.
[93] F La Rue, above.
[94] F La Rue, above.
[95] N Galvin, '*Just hook it into our veins'*, *The Sydney Morning Herald*, 21 October 2012, http://www.smh.com.au/digital-life/digital-life-news/just-hook-it-into-our-veins-20121018-27s6e.html, (viewed 28 August 2013).
[96] T Leaver, quoted in N Galvin, above.
[97] New Zealand Law Commission, note 81, p 42.
[98] New Zealand Law Commission,above.
[99] New Zealand Law Commission, above.
[100] New Zealand Law Commission, above.
[101] New Zealand Law Commission, above.
[102] J,Donath, 'Identity and deception in the Virtual Community' in M Smith and P Kollock (eds), *Communities in Cyberspace* (1999), p 45.
[103] A Cox, 'Making Mischief on the Web', *Time Magazine*, 16 December 2006, http://www.time.com/time/magazine/article/0,9171,1570701,00.html (viewed 28 August 2013.
[104] Human Rights Committee, *General Comment No. 34*, note 4, para 11.
[105] New Zealand Law Commission, note 81, p 119.
[106] New Zealand Law Commission, above, p 101 (quoting a submission from Judge D Harvey).
[107] *La Ligue Contre La Racisme et L'Antisemitisme (LICRA) and Union Des Etudiants Juifs De France (UEJF) v. Yahoo! Inc. and Yahoo France* (20 February 2002). For a general discussion of this case in English, see I Nemes, 'Regulating Hate Speech in Cyberspace: Issues of Desirability and Efficacy' (2002) 11(3) *Information & Communication Technology Law* 193, pp 202-203.
[108] *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 7 November 2001, Case Number C-00–21275 JF, Docket No 17.
[109] The *Sex and Age Discrimination Legislation Amendment Act 2011* (Cth) amended the SDA to expressly provide that the Division relating to sexual harassment (Div 3 of Part II) applies 'in relation to acts done using a postal, telegraphic, telephonic or other like service (within the meaning of paragraph 51(v) of the Constitution).' The Explanatory Memorandum to the Amending Act stated that the power in paragraph 51(v) of the Constitution 'has gained significant relevance in the context of sexual harassment given the ubiquity of new technologies such as social networking websites, e-mail, SMS communications, and mobile telephone cameras.'
[110] *Racial Discrimination Act 1975* (Cth) s 9 (emphasis added).
[111] *Racial Discrimination Act 1975* (Cth) s 18C.
[112] *Jones v Toben* [2002] FCA 1150 (the judgment in this case was upheld on appeal: see *Toben v Jones* (2003) 129 FCR 515).
[113] *Racial Discrimination Act 1975* (Cth) s 18(D).
[114] *Racial Discrimination Act 1975* (Cth) s 17.
[115] See J Hunyor, 'Cyber-racism: can the RDA prevent it?' (2008) 46 *Law Society Journal* 34, pp 34-35.
[116] J Hunyor, above, p 35.
[117] J Hunyor, above, p35.
[118] See J Swift, 'Bains Cohen takes on Facebook in internet bullying case', *The Lawyer*, 12 June 2012. At http://www.thelawyer.com/bains-cohen-takes-on-facebook-in-internet-bullying-case/1012919.article (viewed 28 August 2013).
[119] *Broadcasting Services Act 1992* (Cth), Schedule 5.
[120] *Criminal Code Act 1995 (Cth)* s 474.17.
[121] See Joint Select Committee on Cyber-Safety, Parliament of Australia, *High-Wire Act: Cyber-Safety and the Young* (2011), pp 305-7, 313-324. At

http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jscc/report.htm (viewed 28 August 2013).

[122] *Work Health and Safety Codes of Practice 2011: How to manage work health and safety risks*. At http://www.comlaw.gov.au/Details/F2011L02804 (viewed 28 August 2013).

[123] *Work Health and Safety Codes of Practice 2011*, above, at 1.2 and 2.1.

[124] WorkSafe Victoria, *Your guide to workplace bullying – prevention and response* (October 2012), p. 2. At http://www.worksafe.vic.gov.au/__data/assets/pdf_file/0008/42893/WS_Bullying_Guide_Web2.pdf (viewed 28 August 2013).

[125] Department of Commerce, *Bullying and violence: frequently asked questions* (see question 7: What are the duties of the employer under the Act in relation to bullying?), http://www.commerce.wa.gov.au/worksafe/content/safety_topics/Bullying/Questions.html (viewed 28 August 2013).

[126] See *Crimes Act 1958* (Vic), s 21A.

[127] *Criminal Code Act 1995* (Cth) s 474.17

[128] *Broadcasting Services Act 1999* (Cth) schs 5 and 7.

[129] See *Broadcasting Services Act 1999* (Cth) sch 7 ss 20-21 and *National Classification Code 2005* (Cth) items 1(a)-(c).

[130] I Nemes, note 107, pp 204-5.

[131] Australian Law Reform Commission, *Classification- Content Regulation and Convergent Media: Final Report*, Report No. 118 (2012), para 2.24. At http://www.alrc.gov.au/publications/classification-content-regulation-and-convergent-media-alrc-report-118 (viewed 28 August 2013).

[132] Australian Law Reform Commission, above.

[133] *Broadcasting Services Amendment (Online Services) Act 1999* (Cth) schs 5 and 7.

[134] *Broadcasting Services Act 1992* (Cth), Division 4, s 130M.

[135] *Broadcasting Services Act 1992* (Cth), Division 4, s 130N.

[136] *Broadcasting Services Act 1992* (Cth), Division 3, ss 101, 89, 90.

[137] See Australian Law Reform Commission, note 131, para 2.29.

[138] See Australian Law Reform Commission, above, paras 15.42-15.54.

[139] See Australian Law Reform Commission, above, para 16.34.

[140] *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic), ss 57, 57A and 58.

[141] See for example *Crimes Act 1958* (Vic) s 21A; *Crimes (Domestic and Personal Violence) Act 2007* (NSW) ss 7, 8, 13.

[142] *Criminal Code Act 1995* (Cth) Part 10.6, Div 474, Sub-div C.

[143] *Criminal Code Act 1995* (Cth) Part 10.6, Div 474, Sub-div C, s 474.14

[144] *Criminal Code Act 1995* (Cth) Part 10.6, Div 474, Sub-div C, s 474.15

[145] *Criminal Code Act 1995* (Cth) Part 10.6, Div 474, Sub-div C, s 474.16

[146] *Criminal Code Act 1995* (Cth) Part 10.6, Div 474, Sub-div C, s 474.17

[147] See for example the *Communications Act 2003* (UK) ss 32, 127. See also *Chambers v DPP* [2012] High Court Justice Queen's Bench Division Divisional Court Case No CO/2350/2011 (27 June 2012); J, Lawless, 'On-line rants land Facebook and Twitter users in legal trouble', *The Sydney Morning Herald*, 19 November 2012. At http://www.smh.com.au/technology/technology-news/online-rants-land-facebook-and-twitter-users-in-legal-trouble-20121116-29gf7.html (viewed 28 August 2013).

[148] See J Lawless, above.

[149] See J Lawless, above.

[150] J Lawless, above.

[151] K Starmer (Director of Public Prosecutions, UK) quoted in D, Casciani, 'Prosecutors clarify offensive on-line posts', *BBC News UK*, 19 December 2012. At http://www.bbc.co.uk/news/uk-20777002 (viewed 29 August 2013).

[152] Director of Public Prosecutions (UK), *Interim guidelines on prosecuting cases involving communications sent via social media* (19 December 2012), para 12. At http://publicintelligence.net/uk-cps-social-media-guidelines/ (viewed 29 August 2013).

[153] Director of Public Prosecutions (UK), above, para 2.

[154] Director of Public Prosecutions (UK), above, paras 12(4) and 13.

[155] See the offences in the *Criminal Code Act 1995* (Cth) ch 10, pt 10.6, div 474, sub-div F.

[156] See the offences in the *Criminal Code Act 1995* (Cth) ch 10, pt 10.6, div 474, sub-div D.
[157] Joint Select Committee on Cyber-Safety, note 121, para 11.77.
[158] See *Sex and Age Discrimination Legislation Amendment Act 2011* (Cth) s 56, which removed the requirement in s 28F(2)(a) of the SDA that a student who suffers sexual harassment must be an 'adult' student (i.e. 16 or over) for the sexual harassment to be unlawful under the SDA.
[159] See the offences in the *Criminal Code Act 1995* (Cth), ch 10, pt 10.6, div 474, sub-div G.
[160] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, opened for signature 28 January 2003, CETS No. 189 (entered into force 1 March 2006). At http://conventions.coe.int/Treaty/EN/Treaties/Html/189.htm (viewed 28 August 2013).
[161] See the *Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, para 3. At http://conventions.coe.int/Treaty/EN/Reports/Html/189.htm (viewed 28 August 2013).
[162] *Convention on Cybercrime*, opened for signature 23 November 2001, CETS No. 185, (entered into force 1 July 2004). At http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (viewed 28 August 2013).
[163] See also the *Cybercrime Legislation Amendment Act 2012 (Cth).*
[164] *Durban Declaration, adopted at the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance*, (endorsed by GA Resolution 56/266), UN Doc A/CONF.189/12 (2001). At http://www.un-documents.net/durban-d.htm (viewed 29 August 2013). .
[165] *Durban Programme of Action*, *adopted at the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance*, (endorsed by GA Resolution 56/266) (2001), para 145. At http://www.refworld.org/docid/3db573314.html (viewed 29 August 2013).
[166] *World Summit on the Information Society: Plan of Action*, UN Doc WSIS-03/GENEVA/DOC (2003), para 25(c). At http://www.un-documents.net/wsis-poa.htm (viewed 29 August 2013).
[167] See, for example, Judge S Scholberg, *An International Criminal Court or Tribunal for Cyberspace,* (Paper to the 13th International Criminal Law Congress, Queenstown, New Zealand, 12-16 September 2012). At http://www.crimlaw2012.com/abstract/11.asp (viewed 28 August 2013).
[168] Judge S Scholbery, above, p 2.
[169] Available at http://www.facebook.com/legal/terms (viewed 29 August 2013).
[170] See http://www.cybersmart.gov.au (viewed 29 August 2013).
[171] See http://www.dbcde.gov.au/online_safety_and_security/cybersafetyhelpbutton_download (viewed 29 August 2013).
[172] See http://somethingincommon.gov.au/backmeup (viewed 29 August 2013).
[173] See http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/consultative_working_group (viewed 29 August 2013).
[174] See Joint Select Committee on Cyber-Safety, note 121, Ch 5
[175] Joint Select Committee on Cyber-Safety, above, Recommendation 4, pp xxvii and 151.
[176] Joint Select Committee on Cyber-Safety, above, Recommendation 6, pp xxvii & 163.
[177] Joint Select Committee on Cyber-Safety, above, Recommendation 8, pp xxvii & 174.
[178] Joint Select Committee on Cyber-Safety, above, Recommendation 9, pp xxvii & 174.
[179] Joint Select Committee on Cyber-Safety, above, Recommendation 11, pp xxviii & 175.
[180] Joint Select Committee on Cyber-Safety, above, Recommendations 21 and 22, pp xxx & 330.
[181] Joint Select Committee on Cyber-Safety, above, Recommendation 23, pp xxx & 335.
[182] Joint Select Committee on Cyber-Safety, above, Chapter 13, pp 355-373, paras13.1-13.55.
[183] New Zealand Law Commission, note 81, pp 14-15.
[184] New Zealand Law Commission, above, p 15.
[185] New Zealand Law Commission, above, p16.
[186] New Zealand Law Commission, above, pp16-17.
[187] New Zealand Law Commission, above, p 18.
[188] New Zealand Law Commission, above, p16.
[189] New Zealand Law Commission, above.
[190] Joint Select Committee on Cyber-Safety, note 121, Recommendation 2, pp xxvi and 63.
[191] Joint Select Committee on Cyber-Safety, above, Recommendation 3, pp xxvi and 117.
[192] Joint Select Committee on Cyber-Safety, above, Recommendation 14, pp xxviii and 263.

[193] Joint Select Committee on Cyber-Safety, above, Recommendation 19, pp xxx and 274.
[194] Joint Select Committee on Cyber-Safety, above, Recommendation 14, pp xxviii and 263.
[195] Joint Select Committee on Cyber-Safety, above, Recommendation 14, pp xxviii and 263.
[196] Joint Select Committee on Cyber-Safety, above, Recommendation 17, pp xxix and 269.
[197] Joint Select Committee on Cyber-Safety, above, Recommendation 18, pp xxix and 272.
[198] Joint Select Committee on Cyber-Safety, above, Recommendation 24, pp xxxi and 430.
[199] Joint Select Committee on Cyber-Safety, above, Recommendation 25, pp xxxi and 438.
[200] Joint Select Committee on Cyber-Safety, above, Recommendation 26, pp xxxi and 438.
[201] Joint Select Committee on Cyber-Safety, above, Recommendation 27, pp xxxi and 464.
[202] Joint Select Committee on Cyber-Safety, above, Recommendation 29, pp xxii and 499.
[203] Joint Select Committee on Cyber-Safety, above, Recommendation 30, pp xxxii and 507.
[204] Joint Select Committee on Cyber-Safety, above, Recommendation 31, pp xxxii and 508.
[205] New Zealand Law Commission, note 81, p 19.
[206] New Zealand Law Commission, above.
[207] New Zealand Law Commission, above, p 20.
[208] New Zealand Law Commission, above.
[209] New Zealand Law Commission, above, p 19.
[210] Note however that articles 9 and 21 of the *Convention on the Rights of Persons with Disabilities,* expressly refer to access to the Internet for people with disabilities, including through the use of accessible formats.
[211] F La Rue, note 9, p 17.
[212] F La Rue, above, p 17.
[213] F La Rue, above, p 19.
[214] F La Rue, above, p 17.
[215] F La Rue, above.
[216] F La Rue, above.
[217] F La Rue, above.
[218] C Hamelink, *Human Rights in Cyberspace*, http://www.religion-online.org/showarticle.asp?title=283 (viewed 29 August 2013).
[219] C Hamelink, above.
[220] C Hamelink, above.
[221] C Hamelink, above.
[222] *World Summit on the Information Society: Plan of Action*, note 166, para 10(c).
[223] *World Summit on the Information Society: Plan of Action*, above, para 9(e).
[224] *World Summit on the Information Society: Plan of Action*, above, para 10(d).
[225] F La Rue, note 9, p 17.
[226] See F La Rue, above, p 18.
[227] F La Rue, above, p 18 (citations omitted).
[228] Australian Human Rights Commission, *World Wide Web Access: Disability Discrimination Act Advisory Notes*, http://humanrights.gov.au/disability_rights/standards/www_3/www_3.html (viewed 29 August 2013).
[229] Australian Human Rights Commission, *Submission to the Joint Select Committee on Cybersafety Inquiry into Cybersafety for Senior Australians* (January 2002). At http://www.humanrights.gov.au/inquiry-cybersafety-senior-australians-2012 (viewed 29 August 2013).
[230] Australian Human Rights Commission, above, para 6.
[231] See, for example, The Hon S Ryan, *Age discrimination and the internet-older people in the 21st century* (Ruby Hutchinson Memorial Lecture, 14 March 2012). At http://www.humanrights.gov.au/news/speeches/ruby-hutchison-memorial-lecture-2012 (viewed 29 August 2013).
[232] S Ross and R G Smith, 'Risk factors for advance fee fraud victimisation' in Australian Institute of Criminology, *Trends & issues in crime and criminal justice No.420* (August 2011). At http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi420.aspx (viewed 29 August 2013).
[233] Australian Crime Commission, *Submission to the Joint Select Committee on Cyber-Safety Inquiry into Cybersafety for Senior Australians* (2012), p 6. At http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jscc/senior_australians/subs.htm (viewed 29 August 2013).

[234] Australian Crime Commission, above.
[235] See Explanatory Memorandum, Cybercrime Legislation Amendment Bill 2011 (Cth), para 1. At http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr4575_ems_ecca7d37-7fb2-4218-9837-da3ab80f531e%22 (viewed 29 August 2013).
[236] Explanatory Memorandum, Cybercrime Legislation Amendment Bill 2011 (Cth), above, para 3.
[237] See, for example, Australian Bureau of Statistics, 'Computer and Internet use by People with a Disability', *4429.0 - Profiles of Disability*, (2009). At http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/4429.0main+features100142009 (viewed 29 August 2013).
[238] F La Rue, note 9, p 4.
[239] F La Rue, above.
[240] *The promotion, protection and enjoyment of human rights on the Internet*, Human Rights Council Resolution 20/8, UN Doc A/HRC/RES/20/8 (2012), para 1. At http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8 (viewed 27 August 2013).