Enhancing Online Security for Children

Claudia Hall provides an overview of the Enhancing Online Safety for Children Bill and its implications for those services that might be caught in its regulatory net.

On 4 March 2015, the Enhancing Online Safety for Children Bill (the ***Bill***) passed the Senate with strong bipartisan support. The Bill attempted to create a coherent framework for dealing with cyber-bullying and remedy gaps in the pre-existing legislation. Advances in technology and an increasing prevalence of computers and smartphones has led to a rise in access to the internet and social media services amongst children, the latter being used by 90 percent of Australian 12 to 17 year olds.[1] This has created an environment where it is easy to make, widely distribute and access cyber-bullying materials, but where removing the same materials is often difficult. The ability to perpetrate cyber-bullying anonymously, and to bully at a distance and remain unaware of the impact on the victim, also contributes to rising instances of cyber-bullying, with one in five Australian 8 to 17 year olds reporting being cyber-bullied in 2014.[2]

framing a case to fall within prohibited behaviour as defined by the Criminal Code Act and bringing a claim often takes too long to effectively prevent dissemination of the material

CURRENT FRAMEWORK

The current cyber-bullying framework is contained in a range of Federal and State legislation covering issues such as stalking, harassment, defamation, criminal incitement of suicide and criminal use of telecommunications services,[3] as well as industry protocols like the 2013 Cooperative Arrangement for Complaints Handling on Social Networking Sites. This piecemeal approach makes it difficult to assess the effectiveness of these laws in preventing cyber-bullying activities, as liability in each case is tied to the particular offence provision and not based on the act of cyber-bullying itself.

The limited application of current legislation to cyber-bullying circumstances became apparent in 2010, with the first successful Australian prosecution of cyber-bullying. In the case, a 21-year-old pled guilty to stalking charges and received only an 18-month community-based order in relation to over 300 SMS and internet messages sent to a 17-year-old who subsequently committed suicide.[4]

Currently, the *Criminal Code Act 1995* (Cth) (***Criminal Code Act***)[5] provides for imprisonment for up to three years for end-users who engage in menacing, harassing or offensive behaviours through a carriage service, but does not extend liability to those who disseminate such material. Further, framing a case to fall within prohibited behaviour as defined by the Criminal Code Act and bringing a claim often takes too long to effectively prevent dissemination of the material. Likewise, the *Broadcasting Service Act 1992* (Cth)[6] imposes criminal liability on Internet Content Hosts (ICH) or Internet Service Providers if they are aware of offensive content hosted on their websites or servers and do not take it down. However, the BSA will provide no legal remedy against an ICH located overseas.

OUTLINE OF THE BILL

The Bill defines cyber-bullying material as material a reasonable person would conclude was likely to have been intended to have the effect of seriously threatening, intimidating, harassing or humiliating a particular Australian child, whether that effect was direct or indirect, for example as a result of the material being shared with third parties.[7]

1 Australian Communications and Media Authority, 'Click and connect: Young Australians' use of online social media' (Quantitative Research Report No 2, Commonwealth of Australia, July 2009) 8.

2 Ilena Katz et al, 'Research on youth exposure to, and management of, cyberbullying incidents in Australia' (Synthesis Report, Social Policy Research Centre, Department of Communications, June 2014) 2. <http://www.communications.gov.au/publications/cyberbullying>.

3 See, eg, *Crimes Act 1900* (NSW) ss 60E, 529, 545B(2); *Crimes Act 1900* (ACT) s 439; *Criminal Code 1983* (NT) s 204; *Criminal Code 1899* (Qld) ss 320A, 365; *Criminal Law Consolidation Act 1935* (SA) s 257; *Criminal Code Act 1924* (Tas) s 196; *Crimes Act 1958* (Vic) s 21A(2); *Criminal Code 1913* (WA) s 345.

4 'Magistrate slams cyber bullies', *The Sydney Morning Herald* (online), 8 April 2010 http://news.smh.com.au/breaking-news-national/magistrate-slams-cyber-bullies-20100408-ru23.html; Alison Caldwell 'Parents welcome ruling on bullying victim's suicide', *ABC* (online), 31 May 2011 http://www.abc.net.au/news/stories/2011/05/30/3231123.htm?site=melbourne.

5 s 474.17, Criminal Code Act. See also: ss 474.14-474.16.

6 s 91.21, BSA.

7 Enhancing Online Safety for Children Bill 2014 (Cth) cl 5(1)-(2).

The Bill governs three main groups: end-users, relevant electronic services and social media services. End-users are individuals who have posted material on relevant electronic or social media services.[8] Relevant electronic services are set out in the Bill and include SMS and MMS, email, instant messaging and chat services. In contrast, a social media service is defined as an electronic service whose primary purpose is to enable online social interaction, that is the sharing of material for social purposes[9] between two or more end-users or the posting of material and which allows end-users to link to or interact with some other end-users.[10]

Part 2 of the Online Safety Bill creates the Children's e-Safety Commissioner (the ***Commissioner***) and sets out their functions and powers. The Commissioner will be an independent statutory office within the Australian Communications and Media Authority (***ACMA***), acting as an accessible, centralised point of contact for online safety issues for industry, Australian children and those charged with their welfare.[11] The Commissioner's key functions, will be administering the proposed complaints system in part 3 and the scheme for the removal of cyber-bullying material from large social media sites in part 4, as well as promoting education about cyber-bullying and coordinating existing initiatives tackling cyber-bullying.[12] The Commissioner would also administer the online content scheme in schedules 5 and 7 of the BSA, previously administered by the ACMA.[13]

Part 3 of the Bill establishes a complaints system for cyber-bullying material targeted at an Australian child, whether through a relevant electronic service or a social media service. Complaints can be made to the Commissioner by the child, by their parent or by other authorised persons.[14] The Commissioner will have the power to investigate complaints and conduct such investigations as they see fit.[15] However, the Commissioner can only request or require that a social media service remove the material if the child can provide evidence it was already the subject of a complaint under the service's complaints scheme.[16]

Part 5 of the Bill gives the Commissioner the ability to issue end-user notices if satisfied the material is cyber-bullying material targeted at an Australian child posted on a relevant electronic or social media service by that end-user.[17] End-user notices can require the removal of the material from the service, refraining from posting cyber-bullying material targeting that child or apologising.[18] These notices are enforceable by injunctions but not by penalty provisions.[19]

THE TWO-TIERED SCHEME

The Bill creates a two-tiered voluntary scheme in relation to notice and compliance requirements for large social media services.

Becoming a tier 1 service is voluntary and as long as social media services meet basic safety requirements by including a statement against cyber-bullying in their terms of service, creating a complaints system and ensuring they have a designated contact person for the purposes of the Bill,[20] the Commissioner cannot refuse their application to become a tier 1 service. In contrast, while a social media service can volunteer to be a tier 2 service, they can also be declared a tier 2 by the Commissioner in certain circumstances.[21]

the Commissioner can only request or require that a social media service remove the material if the child can provide evidence it was already the subject of a complaint under the service's complaints scheme

Both tier 1 and tier 2 services may receive notices requesting them to remove cyber-bullying material provided on their service in the next 48 hours, if the affected child has already made a complaint about the material through the service's complaint scheme and the material was not removed within 48 hours of that complaint.[22] However, such notices only bind tier 2 services, which will be subject to injunctions, enforceable undertakings or civil penalties of up to $17,000 a day if they do not comply with the notice to the extent they are capable of doing so.[23] Tier 1 services, or any service that is not 'large', can ignore these requests without legal ramifications.[24]

>

8 Ibid cl 4 (definition of 'relevant electronic service').
9 Ibid cl 9(2).
10 Ibid cl 9.
11 Explanatory Memorandum, Enhancing Online Safety for Children Bill 2014 (Cth) 3.
12 Enhancing Online Safety for Children Bill 2014 (Cth) cl 15.
13 Ibid cl 15(1)(a)(ii).
14 Ibid cl 18(1), (2).
15 Ibid cl 19.
16 Ibid cl 18(4), (5).
17 Ibid cl 42.
18 Ibid cl 42(1)(e)-(g).
19 Ibid cls 43, 48.
20 Ibid cl 23.
21 Ibid cl 30.
22 Ibid cls 29, 35.
23 Ibid cl 36.
24 Ibid cls 31(3)(a), 35-36.

Enhancing Online Security for Children [CONT'D]

> While requesting instead of requiring removal of material seems inadequate, it is likely that this is an attempt to circumvent the enforcement issues that arise when trying to hold overseas services liable for breaches of Australian legislation.[25]

The Bill creates a two-tiered voluntary scheme in relation to notice and compliance requirements for large social media services.

Thus, as the impact of being a tier 2 service is significant, it is important to understand the mechanisms through which a social media service can be declared a tier 2 service.

A social media service that has not signed up for the scheme can be declared a tier 2 if:

- the service is a large social media service;
- within the last 28 days the Commissioner gave the service provider a written invitation to apply to be a tier 1 service, and they did not apply; and
- the Commissioner believes the service does not comply with the basic online safety requirements.[26]

A social media service that was formerly a tier 1 service can be declared a tier 2 service if:

- its tier 1 status is revoked, which requires that:
  - the social media service has been a tier 1 service for more than 12 months; and
  - in the last 12 months, they have repeatedly failed to comply with the Commissioner's notice requests; or
- the Commissioner is satisfied the service does not comply with the basic online safety requirements;[27]
- the service is a large social media service; and
- the Commissioner believes the service should be declared a tier 2 service, considering their compliance with basic online safety requirements, the revoking of their tier 1 status and any other relevant matters.[28]

Therefore, if a service believes they could be large and thus be covered by the Bill's enforceable provisions, volunteering to be a tier 1 service provides a number of benefits.

First, if the service has complied with basic online safety requirements, volunteering to be a tier 1 service allows a 12-month period during which the service will be exempt from being subject to penalty provisions if it fails to comply with the Bill.[29] Secondly, if a service volunteers to be a tier 1 service it has the option of having its definition of cyber-bullying material (found in their terms of use) replace the Bill's definition for the purpose of the Commissioner's assessment of whether particular material is cyber-bullying material.[30] This allows the tier 1 service to shape their own liability and reduce any ambiguity about what will and will not constitute cyber-bullying on their site.

INTERPRETATION ISSUES

A number of issues arise when considering how the provisions of the Bill as they currently stand would be applied in practice.

Firstly, the Bill does not make it clear exactly what constitutes a social media service. The explanatory memorandum refers to services such as Facebook, Google, Yahoo7! and Microsoft as social media services.[31] However, a 2014 study found that 11% of cyber-bullying was carried out on Snapchat, 10% on Ask.fm and 5% on Skype.[32] It is arguable that the primary purpose of these services is to enable online social interaction between two or more end-users, making them social media services, despite the fact that they are more likely to only involve interaction between two users. Further, it is possible the definition could extend to include user forums such as those on Yahoo7! Answers. As such, the Bill's wide drafting makes it difficult to determine what services will be caught by its provisions, further complicating compliance.

This leads to the second issue of why only social media services, as distinct from relevant electronic services, are subject to the Bill's enforceable penalty provisions. If a service like Skype is held to be a social

25 Explanatory Memorandum, Enhancing Online Safety for Children Bill 2014 (Cth) 42, 82. This issue also arises under the BSA s 91.
26 Enhancing Online Safety for Children Bill 2014 (Cth) cls 23, 31(4).
27 Ibid cl 25.
28 Ibid cl 31.
29 Explanatory Memorandum, Enhancing Online Safety for Children Bill 2014 (Cth) 4.
30 Enhancing Online Safety for Children Bill 2014 (Cth) cls 23(3), 29(2).
31 Explanatory Memorandum, Enhancing Online Safety for Children Bill 2014 (Cth) 32.
32 Ibid 17.

media service under the Bill then it is unclear why services like iMessage or FaceTime, which also enable social interaction between two end-users should be treated differently, merely because they fall under the categories of instant messaging or chat services which the Bill deems to be relevant electronic services. Recent studies have suggested that cyber-bullying by phone, such as that in the Melbourne case discussed above, or on instant messaging services is just as serious as that undertaken on social media services.[33] The Bill's arbitrary distinction between social media and relevant electronic services is even more confusing given that the Bill governs the latter in other clauses.

While it is arguable relevant electronic services would be more difficult to police under the scheme, as materials posted on them and their complaints schemes are often less public, the Bill only requires that social media services create a complaints system and include a statement against cyber-bullying in their terms. Thus, similar requirements could be imposed on relevant electronic services, especially email and instant messenger services, with minimal difficulty.

Lastly, what constitutes a *large* social media service is not defined. Instead, the determination is left at the Commissioner's discretion, as long as he has regard to the number of users who are Australian residents and Australian children.[34] This makes it difficult for social media services to determine whether they could be subject to the Bill's tier scheme and penalty provisions, and therefore whether they should sign up to the Bill's scheme at all, as if they are not large the obligations imposed by the Bill are unenforceable. While it is possible the ambiguity was intended to incentivise electronic services to uphold the Bill's provisions in case they are found to be large and in breach, given the significant penalties it is preferable there be clarity as to which services are likely to be covered.

COMPARISON TO OTHER JURISDICTIONS

Cyber-bullying is dealt with in various ways in the international context. In the USA, while electronic harassment is governed in 48 states, in the context of cyber-bullying liability is almost always dependent on the effect the behaviour has on a student's ability to participate at school.[35] The UK model is similar to the Australian status quo, dealing with cyber-bullying not through specific laws but through laws governing harassing, menacing and threatening communications.[36]

The most relevant international comparison is New Zealand, which in 2013 proposed the Harmful Digital Communications Bill, which has not yet been enacted, but looks set to pass in 2015.

The Bills are similar in a number of ways, such as their requirement that an informal resolution be attempted,[37] and their inclusion of safe harbour provisions for content hosts that are not notified of a complaint.[38] However, the New Zealand Bill differs from the Australian Bill in its application, the range of available orders, and in its clarity of expression.

if a service believes they could be large and thus be covered by the Bill's enforceable provisions, volunteering to be a tier 1 service provides a number of benefits

The New Zealand Bill's application extends beyond minors and cyber-bullying[39] to Internet Protocol Address Providers (IPAP), such as Vodafone.[40] The New Zealand Bill also provides for a larger range of orders such as taking down cyber-bullying material, posting a correction or forcing an IPAP to release the identity of an anonymous communications author.[41]

The New Zealand Bill also sets out a balancing act for use when making discretionary orders clarifying when orders might be made against an ICH, allowing them to assess the adequacy of their cyber-safety policies against tangible criteria. This balancing act considers: the content and level of harm caused; whether the communication was intended to cause harm; the context and subject matter of communication; the extent to which the communication has spread beyond the original parties;

>

33 Barbara Spears et al, 'Research on youth exposure to, and management of, cyberbullying incidents in Australia. Part A: Literature review (Research Report, Social Policy Research Centre, UNSW, Department of Communications, June 2014) 23; Amy Barnes et al, (2012) 22(2) *Australian Journal of Guidance and Counselling* 206, 215; Yoshito Kawabata et al, 'Forms of aggression, social-psychological adjustment, and peer victimization in a Japanese sample: The moderating role of positive and negative friendship quality' (2010) 38 *Journal of Abnormal Child Psychology* 471; Justin W Patchin and Sameer Hinduja, 'Bullies move beyond the schoolyard: A preliminary look at cyberbullying' (2006) 4 *Youth Violence and Juvenile Justice* 148.

34 Enhancing Online Safety for Children Bill 2014 (Cth) cl 31(8).

35 See: http://www.stopbullying.gov/laws.

36 *Harassment Act 1997* (UK), *Malicious Communications Act 1988* (UK), *Communications Act 2003* (UK) s 127, *Public Order Act 1986* (UK), *Obscene Publications Act 1959* (UK); *Education and Inspections Act 2006* (UK); Magdalena Marczak and Iain Coyne, 'Cyberbullying at School: Good Practice and Legal Aspects in the United Kingdom' (2010) 20(2) *Australian Journal of Guidance & Counselling* 182, 188.

37 Harmful Digital Communications Bill 2013 (NZ) cls 11(1), 12(2)(a); Enhancing Online Safety for Children Bill 2014 (Cth) cl 19(4)-(5).

38 Harmful Digital Communications Bill 2013 (NZ) cl 20(1)(b)(i); Enhancing Online Safety for Children Bill 2014 (Cth) cls 29, 35.

39 Harmful Digital Communications Bill 2013 (NZ) cl 4 (definition of 'digital communication').

40 Ibid cl 17(2A).

41 Ibid cl 17(1)-(2A).

Enhancing Online Security for Children [CONT'D]

the age of the affected individual and the technical practicalities of an order.[42]

Therefore when considering the two Bills, the failure of the Australian Bill to address cyber-bullying attacks perpetrated by phone or instant messaging services; and to set out criteria for use by the Commissioner when deciding whether, and what kind of, order should be made, are significant oversights.

CONCLUSION

While the attempt to create a coherent framework to tackle cyber-bullying is admirable, the Bill arguably manages to overreach in its scope and definitions, and be toothless in its actual application, especially in relation to its enforcement provisions. The Bill also suffers from a number of interpretational issues that limit its usefulness, beyond merely being a signal of the Australian public's intolerance for cyber-bullying. In that regard, the Bill would benefit from a clearer indication of what services exactly it covers, what factors the Commissioner will use when determining whether content is cyber-bullying material and what orders will be used to counteract it, as well as by an expansion of its tier system to include relevant electronic services.

CLAUDIA HALL is a student at the University of Sydney and a paralegal at Allens. This article represents the views of the author only and does not represent the interests of any organisation.

42 Ibid cl 17(4).

CAMLA Young Lawyer Event and Essay Winners – Report by Alexandra Gilbert

For the third time in as many years, CAMLA held its Young Lawyers Networking Event which was proudly organised by the CAMLA Young Lawyers Committee. The winners of CAMLA's annual essay writing competition were also announced. The event was held on 17 February 2015 at Clayton Utz in Sydney and was attended by approximately 100 aspiring young lawyers with a keen interest in communications and media law. It was an inspiring and informative night culminating in relaxed networking drinks overlooking Sydney Harbour.

The CAMLA Young Lawyers Committee gathered a diverse panel of speakers to discuss their career progression and provide personal and professional insights from life in the industry. The panel comprised Michael Cameron (National Editorial Counsel, News Corporation Australia), Fiona Lang (Chief Operating Officer, BBC Worldwide ANZ), Leanne Norman (Partner, Banki Haddock Fiora) and Matthew Lewis (Barrister, 5 Wentworth Chambers) and was moderated by Hugh Brolsma (Senior Associate, Clayton Utz).

In addition to insights from the impressive panel, the event was an opportunity to celebrate the CAMLA essay competition winners which were selected from a record number of entrants. CAMLA President, Page Henty, presented awards to Sadaat Cheema of Clayton Utz, Ian Richards of The College of Law and Matthew Boyley of the University of New England. A selection of entries will appear in upcoming issues of CAMLA's Communications Law Bulletin.

View pictures of the event here:

http://tiny.cc/7zvbux

(thank you to Mandy Chapman, Beyond International for taking these)
Report by Alexandra Gilbert, Corporate Counsel, Bauer Media