MEAA Media submission to the Senate Legal and Constitutional Affairs References Committee's inquiry into the adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying

December 21 2017

Phone Web

PO Box, 723 Strawberry Hills NSW 2012 1300 656 513 MEAA.org

About MEAA Media

The Media, Entertainment & Arts Alliance (MEAA) is the union and industry advocate for Australia's creative professionals. The MEAA Media section includes journalists and others who work in the media industry.

Journalist members of MEAA Media are bound by MEAA's *Journalist Code of Ethics*.

www.meaa.org

Introduction

The Media section of MEAA (hereafter MEAA) welcomes this opportunity to assist the inquiry.

MEAA is concerned at the rise of hate speech in Australia. For example, when Part IIA was introduced into the *Racial Discrimination Act in 1995* it was long before the widespread use of digital technology. Now there are a multitude of platforms available for the widespread dissemination of opinions and messages of all kinds.

Of particular concern, social media platforms enable those engaging in hate speech to spread their message, call others together who share their views and to use these platforms to target and discriminate against individuals and groups on the basis of race.

Journalists and social media

MEAA members are required to engage with the public in numerous ways. Initially, this is through contacting sources and recording them for a news story. The dissemination of news through publishing or broadcasting story is a second method of engagement. In the past this sometimes gave rise to follow-up contact with the audience responding to stories – in the past via mail or telephone. It could even be as simply as talkback radio or letters to the editor.

But the development of digital social media platforms has introduced a new significant way for journalists and the audience to interact. Social media has allowed individuals to speak directly to journalists.

This change has been embraced by media employers who now insist that their employees use social media platforms to promote and engage with audiences in order to build traffic around digital news stories. Indeed, the number of hits on a news story has become a new and even somewhat oppressive key performance indicator imposed on journalists (on top of demands to file more words, with fewer errors, for immediate publication on the media outlet's web site in advance or publishing or broadcasting on traditional media).

In many cases, journalists are being compelled by their employers to express opinions regarding news events, the news stories they are working on and other news stories by developed by their media employer – all with the aim of interacting with an online audience, driving engagement and building traffic numbers to impress advertisers.

It is the nature of social media that heated discussion takes place, often without reference to facts or objectivity, and often with too great a willingness to allow debate to become personal, abusive and threatening. The fact that many social media users depend upon and even thrive on such abuse, often within the veil of anonymity, leaves many journalists exposed to quite horrifying cyberbullying.

Journalists are, by their nature and by the requirements of responsible journalism, accessible to the public. They usually engage openly, using their own names, in order to make social media the tool for increasing audience responsiveness – exactly the sort of increase in "eyeballs" on news stories that media employers demand of their journalist employees.

As outlined above, the nature of journalists' contact with their audience on digital media platforms, including via social media, makes them particularly vulnerable to cyberbullying. As part of their employment they must openly engage with the audience which, in return, may hurl abuse and threats at them – again, often under the protection of anonymity.

MEAA welcomes the opportunity to create a response to this growing problem.

Harassment

MEAA notes that this inquiry stems in part from the Australian Law Reform Commission June 2014 final report: *Serious Invasions of Privacy in the Digital Age*. In section 15 of the report focussing on harassment, the report recommends action be taken about harassment, defining it this way:

> *Harassment involves a pattern of behaviour or a course of conduct pursued by an individual with the intention of intimidating and distressing another person ...*[1]
>
> *Harassment involves deliberate conduct. It may be done maliciously, to cause anxiety or distress or other harm, or it may be done for other purposes. Regardless of the intention, harassment will often cause anxiety or distress. Harassment also restricts the ability of an individual to live a free life*.[2]

The report recommended the enactment of a harassment tort if a privacy tort is not enacted:

> *Generally, a new harassment tort should capture a course of conduct that is genuinely oppressive and vexatious, not merely irritating or annoying. The tort should be confined to conduct that is intentionally designed to harm or demean another individual*
>
> *A harassment tort should also be the same throughout the country. The states and territories should therefore enact uniform legislation, if the Commonwealth does not have the Constitutional power to enact a harassment tort.*[3]

The report acknowledged the role of cyberbullying carried out against children:

> *At present, Australian law does not provide civil redress to the victims of harassment. There is some protection in defamation law, as well as the torts of battery or trespass to the person where conduct becomes physically threatening or harmful. If bullying or harassment, including cyber-bullying, occurs on school property within school hours, a school may be liable under the law of negligence on the basis of a non-delegable duty of care*.[4]

The report did not pay particular attention to the impact of cyberbullying by adults and directed at adults although the report did cite a submission from the Guardian media group concerning how cyberbullying affected journalists:

> *Guardian News and Media Limited and Guardian Australia submitted that it would be preferable to introduce the new privacy tort than modify existing laws relating to harassment. Their submission raises the concern that a harassment tort does not involve a public interest balancing test, unlike the new privacy tort. Given this, they consider that there is '[s]ignificant potential for an harassment style of action or crime to significantly impact on bona fide journalistic activities'.*

With regard to criminal remedies for harassment, the report noted the Commonwealth *Criminal Code*'s sections 474.15 (threats to kill or to harm with penalties of imprisonment for 10 or seven years respectively; and proof of actual fear not being necessary) and 474.17 (using a carriage service to menace, harass or cause offence with a penalty of imprisonment for three years). The report noted that there was a general lack of awareness of the relevant provisions and of the penalties that existed and that this had led to very few actions being brought under the Code. It added:

> *In consultations the ALRC heard concerns raised that state and territory police may be unwilling or unable to enforce criminal offences due to a lack of training and expertise in Commonwealth procedure which often differs significantly from state and territory police procedures.*[5]

With reference to cyberbullying *per se*, the report said:

> *The Department of Communications outlined three options for reform to s 474.17. First, to retain the existing provision and implement education programs to raise awareness of its potential application. Second, to create a cyber-bullying offence with a civil penalty regime for minors. Third, to create a take-down system and accompanying infringement notice scheme to regulate complaints about online content.*[6]

The lived experience of many MEAA members working in the media industry is of being regularly subjected to harassment, abuse and threats on social media[7], where existing laws are not enforced and where there are gaps in the current legislative regime.

The Criminal Code

The relevant section 474.17 contained a penalty of up to three years imprisonment. However, as the ALRC report found, there is very little knowledge or understanding of this section of the Code.

MEAA believes that there is a great need for education in the broad community for the harm associated with cyberbullying and the penalties that can arise through section 474.17.

MEAA also believes that social media platform providers must take responsibility to ensure that their services are not used in such a way as to breach section 474.17. The proliferation of social media platforms and the manner in which they are co-opted to become tools for the dissemination of hate speech and "fake news" means they have a responsibility to police their products in order to ensure they are not being misused as cyberbullying weapons.

Social media platforms

This debate around responsible operation of social media platforms is already somewhat underway as leading social media platforms address the spread of misinformation and "fake news", and interfere in the 2016 US presidential election:

> *"What they did is wrong and we are not going to stand for it. You know that when we set our minds to something we're going to do it".* – Facebook CEO Mark Zuckerberg on the Russian-influence on the US presidential campaign.[8]

The acceptance by social media platforms that they have been responsible for spreading untruths and misinformation, and have allowed their products to become tools to hijack and inflame debate through deception and/or abuse, should also lead them to accept that they have a role as the carriers in question that are being harnessed to allow cyberbullies to spread their harassment, menace and abuse.

> *Facebook plans to double the number of staffers focused on safety and security issues next year to 20,000, up from its current headcount of 10,000, which the social network says includes its "partners."*

Social media carriage services must be part of the solution to the cyberbullying problem – both through education of their users, far greater monitoring efforts to identify cyberbullies and take down offending content in an expeditious manner; and cooperation with the authorities to "take down" cyberbullying communications, securing evidence, and ensuring the prosecution of offenders.

> *Facebook said on Wednesday that it was removing 99 percent of content related to militant groups Islamic State and al Qaeda before being told of it, as it prepared for a meeting with European authorities on tackling extremist content online.*[9]

This will require the substantial cooperation of social media platform companies. But as the US example shows, the social media companies can dedicate considerable effort to stamp out deliberate misinformation campaigns on their platforms. They must also be called to account and respond to cyberbullying which is far more prevalent and easier for them to locate and identify.

> *Freedom of expression means little if voices are silenced because people are afraid to speak up. We do not tolerate behavior that harasses, intimidates, or uses fear to silence another person's voice. If you see something on Twitter that violates these rules, please report it to us.*
> *You may not promote violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or disease. We also do not allow accounts whose primary purpose is inciting harm towards others on the basis of these categories*.
>
> *Examples of what we do not tolerate include, but is not limited to, behavior that harasses individuals or groups of people with:*
>
> - *violent threats;*
> - *wishes for the physical harm, death, or disease of individuals or groups;*
> - *references to mass murder, violent events, or specific means of violence in which/with which such groups have been the primary targets or victims;*
> - *behaviour that incites fear about a protected group;*
> - *repeated and/or or non-consensual slurs, epithets, racist and sexist tropes, or other content that degrades someone.* – Twitter's Hateful Conduct policy[10]

A great concern is how many cyberbullies hide behind anonymity in order to mount their attacks. Efforts should be made by social media platforms to "block" cyberbullying offenders where they can be identified by the platform provider. Obviously encryption and other masking techniques can be utilised to obstruct attempts to locate and identify cyberbullies but vastly improved efforts should be made to "take down" offensive communications and block those responsible.

> *The consequences for violating our rules vary depending on the severity of the violation and the person's previous record of violations. For example, we may ask someone to remove the offending Tweet before they can Tweet again. For other cases, we may suspend an account*. – Twitter's Hateful Conduct policy[11]

The question arises whether merely "taking down" offensive material is sufficient and whether the offences and penalties set out in Australian law are being ignored/side-stepped by social media platforms.

There is a considerable body of circumstantial evidence of victims of cyberbullying are dissatisfied with the efforts of social media platforms to take legitimate action to ensure the offending ceases and the perpetrators are punished in some fashion. If the platforms are not willing to monitor and police their product themselves and provide proper protections for victims of cyberbullying then the law of the land should apply.

Enforcement

Consideration must be given to ensure that the *Criminal Code* is upheld.

Moreover, there should be an examination of overseas jurisdictions to best inform a robust approach to the problem.

New Zealand, for example, has enacted the *Harmful Digital Communications Act* 2015. This Act introduced a civil regime as well as criminal offences with regard to cyber abuse. The Act established a statutory body known as Netsafe to administer the civil regime established under the Act. Under this law, where a digital communication breaches ten communication principles that are set down in the Act, Netsafe, and failing that the Court system, can order the offending material be taken down, order an abuser to publish a correction and/or apology and order that a victim be given the right of reply. Orders can also be made that content hosts to release the identity of anonymous abusers[12]. The Act imposes fines on individuals who breach any court orders in relation to the civil regime[13].

Further, the Act criminalises online abuse where a person intendeds a digital communication to cause harm, it would reasonably expect the person in the position of the victim be harmed and the individual suffers serious emotional distress.[14]

Criminal laws against cyber abuse also exist in a number of US jurisdictions. There have been notable efforts in California, Washington, Utah and New York. We point to these statutes as symbolic of the gravity of the issues before the Committee, rather than an endorsement of their discrete contents.

At an Australian State level, many of the current regimes are deficient. For example, in Victoria single incidents of cyberbullying do not constitute a ”pattern” of behaviour, and many of the current offences in existing legislation require criminal conduct to occur in a “public space” (which may exclude messages sent by direct message.

State legislative regimes need to be examined so as to ensure existing laws are being enforced, and where there are gaps, these are filled by the introduction of new, more relevant and flexible offences.

Education

There will need to be considerable effort on the part of enforcement agencies. But an accompanying education campaign must also educate the community at large. There is little understanding of the harm that cyberbullying can do by the broader community and most likely little or no knowledge of the substantial penalties that exist.

Cyberbullying must be clearly defined and understood in order to stamp it out.

Education must also include reporting mechanisms so that the victims of cyberbullying can quickly flag an offender to both the social media platform and enforcement agencies for follow-up action.

This should be done in cooperation with the Office of the eSafety Commissioner and the Telecommunications Industry Ombudsman.

MEAA believes that our members, as workers in the media industry, should be able to work free from cyberbullying. MEAA will be stepping up efforts with media employers to ensure employers create and operate policies to protect their staff, ensure they work in a safe and healthy environment, that training and counselling regarding with dealing with cyberbullying is made available, and that employers take steps to deal with cyberbullies on behalf of their employees.

Summary

It is clear that while section 474.17 exists, and offers penalties for cyberbullying, it does not readily lend itself to enforcement and is not widely known. As a deterrent, it is failing to keep pace with the widespread use of social media and digital technology generally which is being used as the platform and vehicle for the delivery of hate speech. Cyberbullying can be executed in seconds with only dozen or so characters or an easily-sourced image.

The bullying, abuse, harassment and threats can go on relentlessly from there with the utmost ease and be directed with precision to the intended target's phone, tablet or laptop - at home or at work- 24 hours a day. And because of the nature of social media platforms and the encouragement they give to others to "engage", others can join in so that the abuse can swell and compound as others join the frenzy.

In short, section 474.17 has not kept pace with the rise of offences it seeks to curtail and punish. The tools of cyberbullying are readily available, easily used, allow for anonymous attacks and enable viral assaults.

MEAA believes that while all members of the community are affected by hate speech, and as the ALRC has acknowledged, children can be particularly vulnerable to cyberbullying, journalists are also regularly targeted.

The media of itself is a powerful institution and public interest journalism is vital to a healthy functioning democracy. But the requirements of modern journalism, and the necessity for journalists to engage directly with their audience in order to market/promote their journalism, leaves them particularly exposed to appalling and frequent attacks upon their character, judgment, professionalism and threats to their physical safety.

If journalists are to be compelled to exist as easily-identifiable digital individuals on social media platforms in order to perform their job, and have that engagement measured as a key performance indicator for their ongoing employment, then greater care must be taken to protect journalists from cyberbullying. We stress here that if reforms are supported through this inquiry, that special care be taken in defining journalists such that media practitioners not employed by major media outlets are suitably protected.

In an era where threats to journalists are on the increase (and not helped by politicians who openly attack journalists and their employers using the phrase "fake news" to describe whatever they do not agree with), and dozens of journalists are murdered, assaulted, imprisoned and harassed because of their journalism, government has a responsibility to uphold, protect and promote press freedom and the vital role of public interest journalism.

The tools to arrest the growth of cyberbullying exist but additional effort is needed. In this regard, MEAA acknowledges the Law Council of Australia's submission to the Inquiry at points 9 (as to the range of conduct cyberbullying offences should capture), 10 (the need for proportionality and distinctions between children and adult offenders) and 18(a) (that the law be readily known and available, and certain and clear).

MEAA believes efforts must be increased to identify and report instances of cyberbullying, to educate the community about the threats and penalties associated with cyberbullying, to ensure that the law is upheld and obeyed, and where necessary introduce greater legislative protections (at both a Commonwealth and State level) to assist victims of cyberbullying.

This will require a coordinated effort by:

- Government,
- Social media providers,
- Employers, and
- Enforcement and regulatory agencies.

A coordinated response that focuses on education, monitoring, reporting, and enforcement (including penalties as outlined in the *Criminal Code*) is urgently needed to address this problem.

MEAA looks forward to the Committee's report.

[1] *Serious Invasions of Privacy in the Digital Age*, final report, Australian Law Reform Commission discussion paper, June 2014 https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf
[2] ibid
[3] ibid
[4] ibid
[5] ibid
[6] ibid
[7] See Women in Media Submission (Submission 26) to this Inquiry
[8] "Mark Zuckerberg on Russian election meddling: 'What they did is wrong and we're not going to stand for it'.", Alexei Oreskovic, *Business Insider Australia*, November 2 2017. https://www.businessinsider.com.au/mark-zuckerberg-russia-linked-actions-to-influence-election-were-wrong-2017-11?r=US&IR=T
[9] "Facebook reports progress in removing extremist content", Julia Fioretti, Reuters, November 29 2017 https://www.reuters.com/article/us-facebook-counterterrorism/facebook-reports-progress-in-removing-extremist-content-idUSKBN1DT003?utm_campaign=trueAnthem:+Trending+Content&utm_content=5a1e4ce504d3010887af52bc&utm_medium=trueAnthem&utm_source=twitter
[10] "Hateful conduct policy" Twitter rules, updated November 14 2017 https://support.twitter.com/articles/20175050
[11] ibid
[12] *Harmful Digital Communications Act 2015 (New Zealand) s19*
[13] *Harmful Digital Communications Act 2015 (New Zealand) s21.*
[14] *Harmful Digital Communications Act 2015 (New Zealand) s22.*