Submission to

Environment and Communications Legislation Senate Committee

Enhancing Online Safety for Children Bill 2014

January 2015

Executive Summary

The Australian Interactive Media Industry Association's Digital Policy Group (**DPG**), that represents key digital players including Facebook, Google, Twitter, Microsoft and Yahoo!7, shares the Government's concern to promote and enhance the safety and well-being of young Australians online. This is why we have policies that expressly prohibit bullying; we invest in a reporting infrastructure that allows the millions of people who use our services to report any bullying content to us; we promptly review and action those reports; and, we undertake online safety outreach and awareness-raising.

We also regularly innovate to improve the tools and information that we provide, often based on feedback from governments and child safety experts. For example, Twitter recently announced improvements[1] to its reporting and blocking functionality, part of a longer term strategy to keep Twitter users safe. In addition, nearly four years ago, Facebook began an ongoing collaboration with experts in the fields of human behavior and social interaction from Yale University, University of California, Berkeley, and other schools, in which these experts share what they know about human interaction to help Facebook improve its reporting tools. More information about what the digital industry does to promote the safety and well-being of young Australians is provided in Appendix 1.

Our commitment to the safety and well-being of all Australians and willingness to work with the Australian Government on this important issue is why members of our industry, specifically Facebook, Google, Yahoo!7 and Microsoft, voluntarily entered into arrangements with the Australian Government in 2012 through the Co-operative Arrangements for Complaint Handling on Social Networking Sites[2] (the Protocol).

The DPG welcomes the opportunity to comment on the *Enhancing Online Safety for Children Bill 2014* (the Bill). Based on the experience of the DPG members, who engage with governments and child safety experts around the world, online safety is best achieved when government, industry, and the community work together. Examples of this in other jurisdictions include in the UK where the Government, in response to the House of Commons Culture, Media and Sports Committee's *Online safety: Responses to the Committee's Sixth Report of Session 2013–14, First Special Report of Session 2014–15*,[3] said "The UK Government defends strongly the successful record of the multi-stakeholder model of internet governance where government joins stakeholders from the private sector, civil society and technical community on an equal footing." This came in response to the Committee cautioning against formal regulation of internet content.

In Europe, the digital industry works with government agencies and nonprofits to progress online safety as part of the *CEO Coalition for a Better Internet for Children*.[4] The goal of the coalition is to bring together industry leaders from across the technology industry to exchange

[1] https://blog.twitter.com/2014/building-a-safer-twitter

[2] http://www.communications.gov.au/__data/assets/pdf_file/0004/160942/Cooperative_Arrangement_for_Complaints_Handling_on_Social_Networking_Sites.pdf

[3] *See page 6*, http://www.publications.parliament.uk/pa/cm201415/cmselect/cmcumeds/517/517.pdf

[4] *See,* Creating a Better Internet for Kids: https://ec.europa.eu/digital-agenda/en/creating-better-internet-kids.

best practices and deliver concrete actions on five objectives (reporting mechanisms, age-appropriate privacy settings, content classification, parental controls and effective take down of child abuse material). One direct development from this work is a new tool rolled-out by Facebook called a Support Dashboard, which enables users to track the status of their reports.[5]

The Australian Government's current position to adopt a regulatory approach differs from the UK and European examples cited above. If a government does choose to adopt a regulatory approach, we recommend that the regulation be structured so as to leverage the already considerable investment that the digital industry makes in online safety. The two tiered model outlined in the Bill goes someway towards achieving this. Companies that have a strong online safety track record will be able to apply to become a "tier 1" provider and respond to notices from the Commissioner promptly, the Parliament sets basic online safety requirements for all of the digital industry, and companies that choose not to become a "tier 1" service sit within "tier 2" and are potentially exposed to enforceable orders. This minimises additional regulations on those companies which have already invested and continue to invest in a safety infrastructure by allowing them to apply to become a "tier 1" provider.

Given how important the safety and well-being of young Australians is, it is vital to ensure that any legislation passed is narrowly framed to achieve this. Overly broad legislation runs the risk of penalising Australia's young people for how they communicate and what they say simply because others do not agree with it or find it challenges their sensibilities. We believe that it is important to keep the rights and interests of young people in mind when crafting online safety solutions. As a recent UNICEF Report on *Children's Rights in the Digital World*[6] concluded:

> "If we are to support children's rights, we must find ways of fostering children's right to protection from harm whilst simultaneously empowering them to maximise the benefits of connectivity for their education, health, social connection, economic participation, civic engagement, both as individuals, and as members of their communities. Digital, media, and social literacies are key to enabling children to leverage the benefits of digital media to enact their rights…..In contrast to anecdotal beliefs, children articulated accountability and understanding of the consequences of what they did online, not seeing themselves as vulnerable victims but as sharing the responsibility for making the internet a safe place for themselves and their peers. It is therefore important to support digital literacy initiatives that encourage and empower children to take further responsibility for their online safety."

We now outline our specific comments on the Bill to the Committee for consideration as it formulates its recommendations.

---

[5] *See* Facebook Help Center information about the Support Dashboard: https://www.facebook.com/help/338745752851127.

[6] http://www.youngandwellcrc.org.au/wp-content/uploads/2014/09/Childrens-Rights-in-the-Digital-Age_Report_FINAL.pdf page 13

Specific Comments on the Bill

Definition of cyber-bullying material targeted at an Australian child

We note that the Bill focuses on cyber-bullying content that is considered likely to have the effect on an Australian child of seriously threatening, seriously intimidating, seriously harassing or seriously humiliating the Australian child, as laid out in section 5 (b) (ii).

In our experience, from working closely with child safety experts, this definition is consistent with experts' understanding of what constitutes cyber-bullying. The inclusion of this definition, in our view, will ensure that the legislation is narrowly targeted to focus the harm that it is designed to address and should not have broad, unintended consequences of regulating content, often posted by young Australians, that others find distasteful but is not harmful.

Response Times

To meet the Government's election commitment that the complaint handling scheme enable a fast removal process, the Bill outlines specified removal time frames, as well as language which empowers the Commissioner to extend this period of time on a case by case basis. To ensure that this regulatory scheme continues to leverage the considerable investment that the digital industry makes in enabling the safety and well-being of Australians, particularly young Australians, we believe that these time frames and flexibility are appropriate. We envisage that if any additional reports are made as a result of this scheme, that industry does not already address, it will likely be those reports that involve complex situations that rely on considerable offline contextual knowledge that may take time for both the Commissioner and the service provider to obtain and utilise to process the full nature of the complaint.

Definition of Social Media Service

It is our understanding that the Bill is meant to regulate social media services that enable a user to post content about a child such that the content is viewable by many and, at the same time, it is not possible for the child who is the subject of the content to personally delete the content – where it is an intrinsic element of the service for the content to be broadcast outside the control of the child. The current definition of a "social media service" in the Bill does not squarely capture the services or situations the Bill seeks to regulate and we therefore respectfully suggest that the Committee may wish to consider an alternate definition.

The current definition in Section 9(1)(a) of a "social media service" refers to a service for which "the sole or primary purpose of the service is to enable online social interactions between 2 or more end users." As written, the definition of a "social media service" captures a number of online services that do not provide for public posting of content and do provide opportunities for the child to delete the content. For example, as written, the definition captures communications services such as email, phone calls and text messaging. None of which directly afford the opportunity to publicly post content to many people and all of which allow for removal or deletion of content. We note that any email or text message that is received can be deleted by the recipient.

Additionally, as presently drafted, we are concerned that the Bill requires the Commissioner to assess whether the "**sole or primary purpose"** of the service is to enable online social

interactions. We would like to better understand how will the Commissioner make this determination. For example, will the Commissioner try to make very difficult assessments comparing the number of businesses using a social media platform for business purposes to the number of people using a social media platform for informational or transactional purposes to the number of people using a social media platform for social purposes? Will the Commissioner rely on what others believe to be the primary purpose of the service or what the relevant company believes to be its primary purpose? Moreover, these assessments are made even more difficult by the fact that whether and for what purpose a service is used is not determinative of the harm to the child; the harm to the child arises from harassing content being posted about them on a platform from which they are unable to delete it. Finally, we note that the term "social" in social media can be used to refer to a method of obtaining information, and should not be strictly understood in the sense of socialising. For example, "social technology" is an increasingly common way of discovering information for industry and estimated by McKinsey to be likely to add $900 million to $1.3 trillion to the global economy (*see:* http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_social_economy[AD1]). As a result, numerous forms of digital communication not intended to be covered by the Bill may be found to be for the purpose of enabling online social interaction.

For these reasons, we suggest that the Committee may want to consider a definition of social media services that does not rely on the sole or primary purpose for which people use the service and instead focuses on whether it provides the two components essential to a possible violation of this regulatory scheme. We think that the following definition is useful in defining social network sites for the purposes of this scheme and respectfully request that the Committee give it due consideration:

Any online service, or part thereof, that allows individuals to:

(1) construct a public or semi-public online communication within a bounded system;
(2) articulate a list of other users with whom they share a connection; and
(3) does not include those aspects of an online service from which a person can delete content themselves.

In keeping with this approach we also believe that it is important for clarity that the Bill expressly specifies those 'relevant electronic services' that were not intended to be included within the definition of 'social media services' and would therefore encourage the Committee to expressly exclude enterprise services, gaming platforms, and news sites. Additionally, it should be clear that companies with platforms that allow developers to build, host, and distribute social media services should not be held liable for interactions facilitated by those developers.

We appreciate the efforts of the drafter to clarify that enterprise (business) services are not intended to be within the scope of the Bill, however, we believe this should be expressly contained within the legislative text not within a Note, which leaves open for argument the intent to exclude it. To clarify the reasons why we believe enterprise services should not be in scope, we would expect that a complaint would be required to be raised in the first instance with the network administrator for the enterprise (i.e., the company or school) who sets the use policies for this limited and self-regulated community and also has the administrator rights

not only to remove content but to set in motion consequences for violation of those use policies.

We also suggest that there should be an express exclusion from the Part 4 scheme of gaming platforms and news sites, many of which have social features. Specifically "It is not intended to include online games or online gaming platforms and services that have a communication function (the primary purpose would be to play the game) or news sites which allow readers to comment on articles (the primary purpose would be to provide news to the public)."

Lastly, given the inextricable connection between the intent of the bill and the definition of a social media service we are concerned that it is possible, as presently drafted, for the Minister to employ an update in regulations such that *any* electronic service could be deemed to be covered by the social media notice and removal scheme in Part 4. The decision to include other communications services such as email or messaging services, which are not public or semi-public communications and can be deleted by the end recipient, within this regulatory scheme, not only significantly expands the scope of the Bill, it fundamentally alters the intent of the Bill and should not occur without proper parliamentary oversight and public debate. We believe that any attempt to include other electronic services such as email or message type services would require considerable re-examination of the intended purpose of this regulatory scheme.

We note that the Department of Prime Minister and Cabinet's *Legislation Handbook*[7] provides guidance on the matters that should be included only in Acts of Parliament, as opposed to rules and regulations. These include "significant questions of policy including significant new policy or fundamental changes to existing policy", "rules which have a significant impact on individual rights and liberties" and "procedural matters that go to the essence of the legislative scheme".[8] In our view, deciding which services are to be subject to a government mandated content removal scheme "are significant questions of policy", which will have "a significant impact on individual rights and liberties", and which "go to the essence of" the proposed regime.

We therefore recommend that subsection 9(1)(b) be deleted and subsection 9(1)(a) be amended consistent with our proposed definition above. Alternatively the government may wish to consider making the regulations contemplated in section 9(1)(b) a disallowable instrument.

Monitoring

Social media services involve the generation of user-generated content that is not necessarily curated or moderated by a central publisher prior to publication. This model of communication leads to important outcomes in terms of allowing individuals to express themselves and engage with a significant number of people from all over the world with different viewpoints and cultures.

[7] http://www.dpmc.gov.au/guidelines/docs/legislation_handbook.rtf
[8] See paragraph 1.12

The volume and value of communication that occurs via digital media and its nature means that proactive monitoring is neither practical or desirable. By way of illustration, over 100 hours of new content is uploaded onto YouTube every minute. Similarly, more than 500 million tweets are posted Twitter daily - 1 billion every two days.

We understand that there is no intention that the proposed scheme impose any obligation on social media services to proactively monitor content.

For the avoidance of doubt we suggest that this be made explicit by insertion of the following provision:

> *For the avoidance of doubt, nothing in [this section] or [Act] requires a social media service to monitor content proactively.*

Section 18 Complaints About Cyber-Bullying

As stated above, if governments choose to regulate this area to which industry already dedicates considerable resources, we respectfully suggest that any regulatory scheme be structured so as to leverage and build on top of industry's own investment and commitment. At present, ***all*** complaints about cyber-bullying can be made to the Commissioner under Section 18, however, requests for removal can only be made under Section 29 after use of the service's own complaint handling scheme.

The provisions as they are currently drafted will result in the acceptance of complaints by the Commissioner that do not meet the necessary threshold of not being actioned by a social media service within the timeframes specified in the legislation.

We suggest that the legislation be amended such that a complaint can only be made to the Commissioner under Section 18 *after* a person has sought to have the content removed using the service's own complaint handling scheme or immediately should a site not have reporting systems. This amendment would minimize inefficiencies created by the Bill as currently drafted, ensure the Commissioner's efforts are put toward possibly actionable complaints, and allow the Government to leverage and build on the digital industry's own considerable commitment to and investment in safety policies and reporting infrastructures.

Additionally, in order to ensure a more efficient and effective handling of actionable complaints we recommend that the Bill should be more specific about the level of detail that the Commissioner must obtain prior to accepting and subsequently referring a complaint to a social media service. For example, that the Commissioner should be required under the legislation to obtain appropriate evidence from a complainant in relation to the age of the complainant, the URL or other online identifiers necessary to swiftly locate the content, and, proof of residential status in Australia by the young person affected.

Finally, again to ensure efficient and fast responses, we respectfully suggest that the Committee consider suggesting amendments to the Bill to Section 39 to require the Commissioner, when considering whether the social media service has failed to take down

cyber-bullying content within a specified timeframe (which then triggers them issuing a social media notice), to take into consideration key factors including the accuracy of the report of abuse, the complexity of the case, whether sufficient evidence has been provided to the social media service to prove that the threshold of 'cyber-bullying targeted at an Australian child', what actions the social media service has taken with respect to the material (including warnings, temporary disconnections) and whether the material has been removed within the timeframes specified in the legislation as per section section 29 (1)(c).. Similarly, factors which should be taken into account in relation to Section 40 -- compliance with a social media notice -- include whether the Commissioner provided appropriate evidence in relation to the age of the complainant, the URL or other online identifiers necessary to swiftly locate the content, any contextual circumstances to confirm the bullying nature of the content if not visible on its face, and proof of residential status by the complainant within Australia.

Self Removal

We note that the action of taking down material by the person who posted potentially cyber-bullying material is a very desirable outcome in that it signals an acceptance by the person who has posted the material that their actions were inappropriate, which should lead to the changes in behaviour that we believe this Bill is intended to achieve.

In cases where it can be confirmed that the potentially cyber-bullying material has been removed by the person who posted that material, we see continued regulatory action for such cases as being unnecessary and an inefficient use of regulatory resources. We suggest that the Committee give consideration to ensuring that the Bill be amended to reflect that the Commissioner should not be required to pursue the variety of actions laid out in the Bill if the content is removed by the individual that posted the material in the first place.

End user notice scheme

We understand that the Government wishes the end user notice scheme in Part 5 to potentially apply to both social media services and private communications, however, we are concerned about how, as a practical matter, the end user notice scheme can be practically implemented. If the person sending the communication is using a pseudonym and is not readily identifiable, then -- depending on the nature of the service -- it may be difficult for the Commissioner to send the notice to that end user. For example, some services operate on a "follow" model which means that you cannot send a direct message to a person unless they follow you (this model was designed as a protective measure to prevent harassment) and the end user in question may not follow the person they are bullying and/or may not follow the Commissioner, so it is unclear how the notice can be delivered. In addition, many online services give end users the choice about the amount of personal details they provide when registering for an account, and so may not have sufficient contact details for the sending of an end user notice, and in any event have clear policies that limit the disclosure of personal information to law enforcement and government agencies.

Extension to external Territories

The DPG notes that Section 46(4), 47(4), 48(4) and 97 specify that the enforcement provisions of civil penalties, enforceable undertakings and injunctions apply to acts, omissions, matters and things outside Australia; or in the case of Section 97 summons may be served on, or given to, body corporates that do not have a registered office or a principal office in Australia.

We are concerned about these provisions. Firstly, because such provisions represent significant overreach with respect to the powers that are held by the Federal Circuit Court of Australia and may at best, not be actionable. We submit that the Bill should be redrafted to reflect the actual limits of the jurisdiction of the Federal Circuit Court of Australia. Secondly, because this sets a standard for other governments to adopt a similar approach which leads to a conflict of laws situation, and adds uncertainty and cost to business. Thirdly, it potentially causes service providers to choose to nominate a contact person who works at the international headquarters for that company, to ensure consistency with international jurisdictional best practice. Finally, in light of the fact that industry has repeatedly demonstrated it's willingness to *work with* the Australian government, it is unclear what the rationale for these provisions are, if the Government is committed to achieving its policy objectives as stated in this legislation.

APPENDIX 1: The Digital Industry's Approach to Safety and Content Management

The digital industry is committed to the safety of the people who use our services. Our industry provides a strong array of resources and tools in support of this goal.

Our Industry's Commitment to Keeping Young People (and everyone else) Safe

User trust is the cornerstone of the services offered by the digital industry.

Our industry offers our services under policies that outline what people can and cannot do via these services.

For example:

- Yahoo!7's Terms of Service http://info.yahoo.com/legal/au/yahoo/utos/en-au/
- Facebook's Statement of Rights and Responsibilities: https://www.facebook.com/legal/terms
- Microsoft's Terms of Use http://www.microsoft.com/info/au-en/cpyright.mspx
- Twitter's Terms of Service https://twitter.com/tos
- Google Safety Centre http://www.google.com.au/safetycenter/

In addition, many of the sites provide a more succinct explanation of the community standards that people must adhere to on the site.

Facebook provides its Community Standards (https://www.facebook.com/communitystandards):

> ❖ Facebook does not tolerate bullying or harassment. We allow users to speak freely on matters and people of public interest, but take action on all reports of abusive behavior directed at private individuals. Repeatedly targeting other users with unwanted friend requests or messages is a form of harassment.

YouTube Community Guidelines (http://www.youtube.com/t/community_guidelines) state:

- Graphic or gratuitous violence is not allowed. If your video shows someone getting hurt, attacked, or humiliated, don't post it.
- We encourage free speech and defend everyone's right to express unpopular points of view. But we don't permit hate speech (speech which attacks or demeans a group based on race or ethnic origin, religion, disability, gender, age, sexual orientation/gender identity, or their status as a returned soldier).
- There is zero tolerance for predatory behaviour, stalking, threats, harassment, invading privacy, or the revealing of other members' personal information. Anyone caught doing these things may be permanently banned from YouTube.

❖ The Twitter Rules state that:

- **Violence and Threats**: Posting specific and direct violent threats are strictly prohibited on Twitter, with warnings and account suspensions enforced. We also encourage users to report such behaviour to law enforcement so that the threat can be properly evaluated and, if applicable, the behaviour prosecuted.
- **Targeted Harassment and Abuse**: Targeted harassment and abuse is not allowed on Twitter. The consequences for engaging in such behaviour include warnings as well as temporary or permanent account suspensions.
- **Private information**: You may not publish or post other people's private and confidential information, such as credit card numbers, street address or Social Security/National Identity numbers, without their express authorization and permission.

❖ Microsoft's Terms of Use say users can't:

- Defame, abuse, harass, stalk, threaten or otherwise violate the legal rights (such as rights of privacy and publicity) of others.
- Publish, post, upload, distribute or disseminate any inappropriate, profane, defamatory, obscene, indecent or unlawful topic, name, material or information.
- Restrict or inhibit any other user from using and enjoying the Communication Services.

❖ Yahoo!'s Terms state:

You agree to not use the Service to:

❖ upload, post, email, transmit or otherwise make available any Content that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable;

❖ harm minors in any way;

❖ "stalk" or otherwise harass another;

To promote compliance with these policies, our industry provides tools that leverage the considerable and engaged communities active on our sites, to let us know when they believe that there are instances of content or conduct that violates our terms. For example:

- Facebook provides report links throughout the site: https://www.facebook.com/help/reportlinks
- Yahoo!7 provides tools to assist in reporting inappropriate or harmful behavior such as our "Report Abuse" flags and the Abuse Help Forms. The "Report Abuse" flags are easily accessible mechanisms that enable a user to notify the customer care teams of a complaint about specific content.
- Twitter provides a How to Report an Abusive User function https://support.twitter.com/forms/abusiveuser
- YouTube provides a flag system that enables a user to click a flag button to report a video which they consider to be inappropriate http://support.google.com/youtube/bin/answer.py?hl=en&answer=118747
- Microsoft has in place simple and easy-to-use reporting mechanisms which enables it to appropriately categorise and address an alleged report of abuse. https://support.microsoft.com/contactus/emailcontact.aspx?scid=sw;en;1671&ws=reportabuse

To review reports that are received via these tools, members of the DPG maintain extensive review teams that operate 24/7 and work to swiftly take appropriate action with reports. We triage complaints dealing with the most serious cases first.

In addition, all members of the DPG continue to innovate and improve on our reporting tools. For example, Facebook introduced an important new tool to assist with greater transparency in identifying the status of a report made via the Support Dashboard and continues to refine its social resolution tools on an ongoing basis.[9]

On Youtube, the Safety Mode is a tool that operates at the family level. Parents are empowered to determine what content they wish their children to be exposed to. By switching on this tool, users have the option of choosing not to see mature content that they or their children may find offensive, even though the content is not against the YouTube Community Guidelines. Videos that have been age restricted will not show up in video search, related videos, playlists, shows and movies. A demonstration of YouTube Safety Mode is available at http://www.youtube.com/watch?v=gkI3e0P3S5E. In a similar manner Microsoft provides the Family Safety Centre http://www.microsoft.com/security/family-safety/default.aspx#Overview.

Yahoo!7 builds accessible safety and privacy features into all its products, including privacy preferences, blocking capabilities, abuse flagging and FAQ safety guides that are product specific (au.safely.yahoo.com/yahoo-products/) and general online safety tips (au.safely.yahoo.com/faq/).

[9] See e.g., https://www.facebook.com/notes/facebook-safety/details-on-social-reporting/196124227075034 *and* https://www.facebook.com/notes/facebook-safety/improved-tools-to-support-your-facebook-experience/473126442708143

To promote awareness of our policies, tools and safety best practice, industry provides help and educational information through specifically designed parts of their sites. For example:

- The Yahoo!7 specialised safety website[10], which contains tools, tips, hints from experts and other information aimed at keeping children and internet users safe online.
- The Google Family Safety Centre[11], which contains safety tips from experts and information about Google's online safety tools.
- The YouTube Safety Centre[12], which contains content from local partners, including the Australian Communications and Media Authority, the Australian Federal Police, Kids Helpline and the Inspire Foundation on topics that include teen safety, and harassment and bullying.
- The Facebook Family Safety Centre, which contains information for parents[13], teachers, [14] and teens[15] on online safety.
- The Twitter Safety Centre[16], which includes resources and information for parents, teachers, and young people, as well as Twitter's policies, guidelines and best practices.
- Microsoft's Safety Centre[17] which gives consumers the ability to put in place family safety settings for Microsoft products[18] and provides a range of different resources and information about online security and safety.

In addition to these initiatives, individual companies undertake their own education campaigns through initiatives such as Facebook's Be Bold Stop Bullying campaign[19], Google's Good to Know[20] initiative and Microsoft's Think U Know program with the Australian Federal Police.

All members also participate in the various awareness weeks organised by Government, such as, for example, Privacy Awareness Week, Safer Internet Day, National Cyber-Security Awareness Week and National Day of Action against Bullying and Violence.

The AIMIA Digital Policy Group launched the Keeping Australians Safe Online[21] resource which outlines the resources provided by Yahoo!7, Google and Facebook and the group has actively

---

[10] http://au.safely.yahoo.com
[11] http://www.google.com.au/safetycenter/
[12] http://support.google.com/youtube/bin/request.py?contact_type=abuse
[13] http://www.facebook.com/safety/groups/parents/
[14] http://www.facebook.com/safety/groups/teachers/
[15] http://www.facebook.com/safety/groups/teens/
[16] https://support.twitter.com/groups/57-safety-security
[17] www.microsoft.com/safety

[18] http://www.microsoft.com/security/family-safety/default.aspx#Products
[19] https://www.facebook.com/beboldstopbullyingau
[20] http://www.amf.org.au/Assets/Files/MEDIA%20RELEASE%20-%20Good%20to%20Know%20Campaign%20helping%20Australians%20stay%20safe%20online.pdf

[21] http://www.aimia.com.au/enews/Industry%20Development/Digital%20Policy%20Group/AIMIA%20Digital%20Policy%20Group%20Keeing%20Australians%20Safe%20Online%20Public.pdf

distributed this within the community. This resource was subsequently revised to include Microsoft and Twitter resources and re-released as part of the Australian Communication and Media Authority Digital Citizens Update on 23 July 2014[22].

Leading members of the digital industry also collaborate with non-profit organisations and associations including The National Association for Prevention of Child Abuse and Neglect (NAPCAN), www.Reachout.com, The Alannah and Madeline Foundation, headspace, Kids Helpline, Bravehearts and Netsafe to receive expert advice about current trends and issues with the safety of young people and to ensure that these important organisations have the relevant information about the safety policies and tools that are available to them.

[22] http://www.cybersmart.gov.au/About%20Cybersmart/Newsroom/News%20Article%20List/2014/07/Cybersmart%20Digital%20Citizen%20update%20puts%20focus%20on%20cyberbullying.aspx