AIMIA

DIGITAL POLICY GROUP

ENHANCING ONLINE SAFETY FOR CHILDREN

DISCUSSION PAPER

SUBMISSION

7 MARCH 2014

The AIMIA Digital Policy Group's Cyber-safety Sub-Group (Cyber-Safety Sub-Group), that represents key digital players including Facebook, Google, Twitter, Microsoft, eBay and Yahoo!7 stands united with the Government in its objective to ensure the safety of Australia's children and young people online.

Debate about cyber-safety policy is not a debate about bullying and censorship but rather about bullying and citizenship.

Members of the Cyber-Safety Sub-Group know and understand cyber-safety issues can have the gravest and most serious impact. Major digital companies have sought to responsibly deal with cyber-safety across every country and culture in the world over many years in the knowledge that good cyber-safety outcomes are good for our users and important to confidence in our industry.

Members of the Cyber-Safety Sub-Group have pioneered this area, investing heavily in sophisticated tools and devoting significant resources to preventing and dealing with cyber bullying. We prohibit bullying behaviour through various mechanisms such as the prohibition of bullying or harassment under our terms of service. We rapidly remove or disable material that relates to bullying or harassment, stalking and intimidation. Our industry has well-established links to, and works closely, with government, child safety organisations and law enforcement agencies.

Key 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[1] (the Protocol). Since the introduction of the Protocol not a single escalation or request to meet with the Australian Government has been received. This suggests that the Protocol is effective and working. We note it is already an offense to engage in online harassment and it is important that the public are educated about existing criminal laws to make sure they are complying with these laws.

Given the Government's commitment to de-regulation and reduction in red tape and lack of evidence that existing mechanisms are not operating as intended, we respectfully submit that the Government should reconsider the proposal to introduce legislation to take down content and rather work to extend the Protocol to apply to more services.

There are also other serious practical concerns with the proposed policy: a rapid take down scheme will at best take five days (much longer than industry's own processes), the possibility that the policy will push children to undertake risky behaviour onto platforms with less highly developed self-regulatory standards and significant likelihood that the laws will be unable to keep pace with technological change.

Lastly, we submit that international best practice and Australian research confirms that prevention, education and empowerment are the most powerful policy levers for producing optimal cyber-safety outcomes here in Australia. More importantly it prevents incidences of bullying before they occur. The Cyber-Safety Sub-Group submits that the Australian government should re-examine existing frameworks including co- or self-

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

regulatory schemes, the already substantive protections under current law (and why there is such a low general awareness of the same) and Government institutions such as the Australian Communications and Media Authority before reaching for more onerous, legislatively backed options including a new Commonwealth cyber-bullying offence.

The Cyber-Safety Sub-Group invites the Australian Government to join the industry in a nation-wide, cross-platform, education and awareness campaign to raise awareness of existing laws and online safety so that those who engage in bullying behaviours and their potential targets know that bullying is not acceptable in our society, by-standers feel empowered to become “up-standers” and speak out, and the Australian public know that there are safeguards and protections in place if needed.

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. In addition key members of our industry have voluntarily entered into a Protocol with the Australian Government which permits escalation of content issues to designated company representatives.

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
- eBay's http://pages.ebay.com.au/help/account/safety.html
- 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. For example, Facebook provides its Community Standards (https://www.facebook.com/communitystandards), YouTube provides the Community Guidelines (http://www.youtube.com/t/community_guidelines) and Twitter publishes The Twitter Rules (http://www.twitter.com/rules).

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, the Cyber-safety Sub-Group members 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 Cyber-Safety Sub-Group members continue to innovate and improve on our reporting tools.

For example, Facebook last year rolled out a new tool to assist with greater transparency in identifying the status of a report made via the Support Dashboard.[2]

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/).

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[3], which contains tools, tips, hints from experts and other information aimed at keeping children and internet users safe online.
- The Google Good to Know site[4] and Safety Centre[5], which contains safety tips from experts and information about Google's online safety tools.
- eBay's Policies Centre[6] which includes information on phishing, protecting personal information and identity theft schemes[7] and Trust and Safety Tutorials[8].
- The YouTube localised Safety Centre[9], which contains content from local partners, including the Australian Communications and Media Authority, the Australian

[2] 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

[3] http://au.safely.yahoo.com

[4] http://www.google.com.au/goodtoknow/

[5] http://www.google.com.au/safetycenter/

[6] http://pages.ebay.com.au/help/policies/overview.html

[7] http://pages.ebay.com.au/help/account/protecting.html

[8] http://pages.ebay.com.au/help/policies/tns-tutorials.html

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[10], teachers,[11] and teens[12]on online safety.
- The Twitter Safety Centre[13], 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[14] which gives consumers the ability to put in place family safety settings for Microsoft products[15] 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[16], Google's Good to Know[17] initiative and, eBay and PayPal's Surf between the Flags[18] 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 recently launched the **Keeping Australian Safe Online[19]** resource which outlines the resources provided by eBay, Yahoo!7, Google and Facebook and the group has actively distributed this within the community.

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), Inspire Foundation, 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.

[9] http://support.google.com/youtube/bin/request.py?contact_type=abuse

[10] http://www.facebook.com/safety/groups/parents/

[11] http://www.facebook.com/safety/groups/teachers/

[12] http://www.facebook.com/safety/groups/teens/

[13] https://support.twitter.com/groups/57-safety-security

[14] www.microsoft.com/safety

[15] http://www.microsoft.com/security/family-safety/default.aspx#Products

[16] https://www.facebook.com/beboldstopbullyingau

[17] http://www.amf.org.au/Assets/Files/MEDIA%20RELEASE%20-%20Good%20to%20Know%20Campaign%20helping%20Australians%20stay%20safe%20online.pdf

[18] http://www.canberra.edu.au/cis/tour/

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

Co-operative Arrangements for Complaint Handling on Social Networking Sites

In January 2013, key members of the digital industry, including Yahoo!7, Facebook, Microsoft and Google voluntarily signed the Co-operative Arrangements for Complaint Handling on Social Networking Sites. Yahoo!7[20], Facebook[21], Microsoft[22] and Google[23] have made self-declarations as to how they comply with the Protocol.

Section 5 of the Protocol provides for a designated and locally based contact person at participating social networking sites that the Australian Government can contact in relation to content issues.

> These providers will have a contact person(s) with whom the Australian Government can discuss issues and any appropriate messaging to the community and media in response to issues as they arise. This is particularly important where an issue is of public interest and as such, requires prompt attention.

To date no such contacts have been made by the Australian Government to the companies who signed the Protocol.

Section 11 of the Protocol also provides that

> providers will meet with government officials on a bilateral basis every six months to discuss trends and emerging issues.

At the time of writing no such meetings have been requested by the Australian Government. This suggests that the Protocol is working and effective and no new issues have emerged.

OTHER CONCERNS

Challenges Facing an E-Safety Commissioner Charged with Implementing a Rapid Take Down Scheme

While we welcome the Government's desire to provide a one-stop-shop and more co-ordinated contact for online safety within government, a legislated scheme will almost always be much slower than industry's own self-regulatory processes when it comes to responding to cyber bullying complaints.

Under the scheme outlined in the Discussion Paper, the process for take down would take at least five days in the unlikely event of no problems or delays being encountered.

When deciding whether to act in relation to a complaint, the e-safety commissioner will need to establish:

[20] http://www.communications.gov.au/__data/assets/pdf_file/0019/161083/Yahoo!.pdf

[21] http://www.communications.gov.au/__data/assets/pdf_file/0004/161077/Facebook.pdf

[22] http://www.communications.gov.au/__data/assets/pdf_file/0017/161081/Microsoft.pdf

[23] http://www.communications.gov.au/__data/assets/pdf_file/0006/161079/Google_YouTube.pdf

a) Age of complainant
b) Location of complainant
c) Whether the complainant is Australian
d) Whether the material can be considered harmful to a child
e) Whether the material is hosted by a large social networking site
f) Whether the material has been referred to a large social networking site
g) Whether the large social networking site has had sufficient time to assess and remove the content
h) Whether the content has been removed, whether the content has now moved to another account or how many other users are not spreading the material

The matter is then referred to the online provider who will need to be permitted time to investigate and respond. The e-safety commissioner will then need to consider the response from the provider and will then need to make a determination. If such a determination is made then the e-safety commissioner will issue the determination to remove content to the online provider.

In comparison, industry processes ensure bullying content is removed rapidly.

Children will undertake risky behaviour on smaller Social Networking Sites with Less Well Developed Protections

The Cyber-Safety Sub-Group notes that the Government's cyber-safety policy does not apply to smaller social media sites despite law enforcement agencies identifying smaller online communications services as their primary areas of concern rather than larger, more responsible sites. The NSW Police have recently indicated that it is the smaller online platforms such as Kik (a real time messaging service provider) that are presenting the most concern[24].

Other examples of smaller communications providers include SnapChat, ask.fm, Chance, Chatroullette and spring.me.

A cyber-safety policy that only targets the larger players, adds redundant regulatory red tape onto responsible companies and will undermine the significant initiatives of major players in the industry.

A policy that clamps down heavily on the things that young people can say to each other on larger responsible sites has potential to drive young people to engage in risk-taking behaviour on services that have less well developed protections in place and are not covered by the legislated scheme.

Material Targeted at and Likely to Cause Harm to an Australia Child

We are concerned that the definition of content that may not be available in Australia is broader than bullying and harassing content.

The standard "material targeted at and likely to cause harm to an Australian child" does not provide the industry or the Australian public with a clear sense of the standard of content removal that is being proposed. Given industry already removes content that bullies and harasses Australian children, we encourage the Government to provide

[24] http://www.smh.com.au/national/police-warning-on-social-media-messaging-app-kik-20131130-2yimo.html

greater clarity around what additional content it believes should be removed and not available in Australia under its proposed scheme.

Government needs to correctly identify what the issue is that needs to be solved

We believe that it is important to correctly identify the problem. It is unclear based on the explanation provided in the Discussion Paper whether Australian parents, teachers and children had tried to use the reporting systems available on all of the large social media platforms, or whether they did not know how to resolve problems that happened online. At the 2013 Australian Government's Cybersafety Summit, the local industry association AIMIA DPG, of which Facebook is a member, undertook a Pop-Up Safety Quiz, which asked how to report content on popular social media sites. The vast majority of these students did not know how to do this. If the problem is that Australians do not know that they can or how to report content on a social media site, then the solution is more education and outreach, rather than legislated content removal.
See, Online Safety Pop-up Quiz: https://www.facebook.com/beboldstopbullyingau/photos/pb.466922616686341.-2207520000.1392883580./599065063472095/?type=3&theater.

Is there a need to introduce a Commonwealth cyber bullying offence?

A clear case for the introduction of a Commonwealth cyber bullying offence has not yet been made.

There are currently extensive criminal and civil remedies that apply to cyber bullying in place in Australia.

The National Children's and Youth Law Centre (NCYLC) has recently reported that

> It is a common misconception that the existing criminal law does not sufficiently cover cyber bullying.[25]

Key Australian laws that provide protection include:

- Civil remedies
  - Tort of defamation[26]
  - Tort of assault (including threats of violence via text, social media)
  - Existing privacy laws including the *Privacy Act 1988*
- Offences that arise from threats that make a person fear personal violence including section 31 of the *Crimes Act 1900* (NSW), section 308 of the *Criminal Code 1899* (Qld), section 163 of *Criminal Code Act 1924* (Tas), section 30 of the *Crimes Act 1900*, section 166 of the *Criminal Code 1983* (NT), section 19(1) to (3) of the *Criminal Law Consolidation Act* (SA)
- Criminal Assault particularly under *Criminal Law Consolidation Act 1935* (SA) which includes actions that threaten by words or conduct
- Stalking laws

[25] http://www.lawstuff.org.au/__data/assets/pdf_file/0099.15030/New-Voices-Law-Reform-Report.pdf paragraph 3.41
[26] http://viralnewschart.com/ShowLink.aspx?linkId=33404256

    - Apply in each state and territory via section 35 of the *Crimes Act 1900 (ACT),* section 545B of the *Crimes Act 1900 (NSW),* section 189 of the Criminal Code 1983 (NT), section 359A of the *Criminal Code 1899 (Qld),* section 19AA of the Criminal Law Consolidation Act, sections 192, 192A of the Criminal Code Act 1924 (Tas), section 21A of the Crimes Act 1958 and Sections 338DD and 338E of the Criminal Code 1913 (WA)
- Criminal Code Act 1995
    - section 474.15 (offence for a person to use a carriage service to threaten to kill or to cause serious harm to another person or a third person)
    - section 474.16 (use of a carriage service to send a hoax communications intending to induce a false believe that an explosive, or a dangerous or harmful substance or that, has been or will be left somewhere)
    - section 474.17 (use of a carriage service to menace, harass or cause offence)
    - section 474.22 (use of a carriage service for child abuse material (eg images of sexual assault)

However one of the most important findings made by the NCYLC is that children are generally not aware that sexting and cyber-bullying is a crime. The NCYLC also report that when children and young people are informed that they face criminal or other charges for such activities it results in the majority being significantly deterred from engaging in these types of activities.

> The prezi has a real effect on young people's behaviour and attitudes, with 68.3% of students saying that they are less likely to engage in sexting and cyber bullying now that they know these actions can be crimes, and 66.3% saying they felt more confident about being able to deal with these issues.

Given the abundance of laws that make cyber-bullying illegal, the Cyber-Safety Sub-Group respectfully submits that more legislation is not the answer. Rather the Australian people, especially its children and young people, will be best served if the Government gives primary focus to the research and education aspects of its online safety election commitment rather than first moving with legislation.

Such an approach would be in keeping with the Best Practice Regulation Handbook (July 2013) (BPR Handbook) including its overall objective of ensuring that the regulatory problem is properly identified in the first instance and that any government response first assesses what other non-regulatory options will efficiently and effectively address the issue before new regulation is pursued.

Alternative Approaches

Cyber-safety requires a team effort combining the collective energy, resources and good will of government, industry and the community.

The digital industry has the benefit of being able to view and assess various cyber-safety schemes throughout the world.

International best practice as well as Australian research in the cyber-safety field demonstrates that prevention, education and empowerment are the most powerful policy levers available to policymakers. More importantly preventative steps reduces the amount of bullying in the first instance. They build resilience in children who may be the victim of bullies and they build a strong and supportive community around potential bullying victims by giving confidence to by-standers to step up and defend others.

Robust education in the fundamentals of digital literacy and citizenship prepares children and young people to interact safely and smartly online regardless of how the technology and platforms may change and where they encounter poor communication.

Simply put education that draws focus to the fact that bullying is not acceptable in our community is the strongest safeguard and protection available to policymakers when contemplating cyber-safety issues. Such training also extends beyond the online world and more broadly into face to face communications and interactions.

The Cyber-Safety Sub-Group submits that the Australian government should examine existing self regulatory frameworks, current laws and Government institutions such as the Australian Communications and Media Authority before reaching for more onerous, legislatively backed options.

The Cyber-Safety Sub-Group invites the Australian Government to join the industry in a nation-wide, cross-platform, education and awareness campaign to raise awareness of cyber-bullying and the laws and Protocols that are already in place so that bullies and their potential victims know that bullying is not acceptable in our society, by-standers feel empowered to stand up and speak out and the Australian public know that there are safeguards and protections in place if needed.