Google Australia Pty Ltd
Level 5, 48 Pirrama Road
Pyrmont NSW 2009
+61 2 9374 4000
www.google.com.au

Google Australia's Submission to the Government's Discussion Paper on Enhancing Online Safety for Children

7 March 2014

EXECUTIVE SUMMARY

Google is pleased to have this opportunity to comment on the Government's Discussion Paper on Enhancing Online Safety for Children. We welcome this initiative by the Government to engage with industry and other stakeholders to consider best practice measures for protecting children online, and we look forward to working with the Government on this important consultation.

Google shares the Government's objective of keeping children safe online. This objective requires ongoing effort. We agree that mechanisms for handling content and cyber bullying concerns quickly are essential, and that children must be able to access assistance with online safety concerns.

In approaching these issues, it is important to keep in mind that there are tremendous benefits of online social networking. Research from the Young and Well CRC (YAW-CRC) has found that "there are a number of significant benefits associated with the use of social networking services (SNS) including: delivering educational outcomes; facilitating supportive relationships; identity formation; and, promoting a sense of belonging and self-esteem. Furthermore, the strong sense of community and belonging fostered by SNS has the potential to promote resilience, which helps young people to successfully adapt to change and stressful events." [1]

Google is committed to online safety

Google believes it is important to support all Australians so that they are equipped and empowered to be capable digital citizens. Being a capable digital citizen is about having the necessary skills to be smart, safe and responsible online. It includes understanding the rights and responsibilities that come with online interactions. Capable digital citizens have the skills and knowledge to take advantage of the opportunities of the online world while minimising the risks.

Promoting digital citizenship is an ongoing effort. We promote digital citizenship through a combination of education, empowerment through user tools, and cooperation between industry, users, government and community organisations.

[1] http://www.inspire.org.au/wp-content/uploads/2011/04/FAQ_CRC1.pdf

Google is highly motivated to work towards a safe and secure environment for our users. This is fundamental to obtaining and maintaining users' trust – which is key to success. In order for a service to be successful, users must feel comfortable using the service. Providers want their brand associated with comfort, safety and security.

Google promotes online safety through a combination of:

- **Policies** - We have strong policies and guidelines in place that set out acceptable content and conduct. Users are warned that postings that breach these policies and guidelines will be removed, and that they may be permanently banned from using the site.
- **Tools** - We have tools in place (such as Google SafeSearch, and Safety Mode for YouTube) that empower people to manage their online experience. We also provide simple and effective ways for users, including young people, to register complaints about inappropriate content or conduct. Industry leading tools such as the YouTube flag system enable users to report content that violates our policies. We respond rapidly to these complaints: we have processes for reviewing complaints from users and other parties - 24 hours a day, seven days a week - and we quickly take action on these complaints, removing content that is found to be in breach of site guidelines/policies.
- **Education** - We provide educational resources such as the Google 'Safety Centre' website (www.google.com.au/safetycenter/) and the YouTube Safety Centre (www.youtube.com/yt/policyandsafety/) to offer advice on how to use Google products in a smart, safe and responsible way. Our product Help Centres provide our users with tips and articles for managing their experience while using Google products and staying safe online.
- **Partnerships** - We partner with NGOs to educate families about cyber safety and develop anti-bullying resources. We invest a large amount of funding, time and other resources in cyber safety initiatives.
- **Cooperation** - We cooperate with governments and law enforcement agencies to address cyber bullying. We are a signatory to the Cooperative Framework on Complaints Handling for Social Media that is in place with the Australian government.

Industry processes address cyber bullying

Google submits that the key challenge in addressing cyber bullying is ensuring that the community is educated to understand that cyber bullying is against the law, and to know what to do if cyber bullying occurs. There are well-functioning laws and industry processes in place to tackle cyber bullying in Australia.

As outlined above, Google has highly developed and effective systems and policies in place. Our policies prohibit the use of our services for harassment and bullying. Also we provide tools that enable users and others to register a complaint regarding inappropriate content. Google responds quickly, and at scale, to notifications from users to remove content that breaches our policies. In addition, we have a range of tools that empower individuals to manage their

interactions with others online. This includes the ability to block another user and to post content privately.

Existing laws already prohibit cyber bullying

Criminal laws in the Commonwealth and every Australian State and Territory already allow cyber bullies to be prosecuted. As the Discussion Paper notes, just one of these laws - s 474.17 of the *Criminal Code Act 1995* (Cth) - has since coming into force in 2005 been used to support 308 successful prosecutions for a broad range of conduct involving the internet, including eight prosecutions involving defendants under 18 years of age. [2]

Raising community awareness that cyber bullying is already a crime

A major reason that there may be a perceived need for 'something more to be done' about cyber bullying is the lack of awareness in the community that cyber bullying is a crime, as well as uncertainty about how to report bullying behaviour when it occurs. As we discuss below, research has shown that merely making young people aware that cyber bullying is a crime can have a real and immediate impact on their behaviour.

Google supports better coordination of cyber safety initiatives

Google supports the creation of a central point of contact and coordination, such as an e-safety commissioner (whether an existing or Associate Member of the ACMA board or an NGO), to be an accessible and central point of contact for the public and industry on matters relating to cyberbullying.

An e-safety commissioner could play an important role in:

- **Coordinating** existing cyber safety resources and initiatives
- **Educating** the community and law enforcement bodies about cyber bullying (the mechanisms and remedies already in place and the nature of Australia's existing laws against cyber bullying)
- **Cooperating** with industry to quickly resolve cases of cyber bullying, building on the existing cooperative framework.

Concerns with legislating mandatory removals

Google has a number of concerns with legislating mandatory removals:

- There is no evidence provided to suggest that a formal legislative process would work better than cooperative industry processes.
- The proposed scheme would not capture many social media sites, including many popular messaging app services commonly used by teenagers. Public expectations regarding the ability of a legislated removals scheme to address cyber bullying are likely to greatly exceed the reality of what such a scheme is capable of achieving.

[2] DP, p 21

- The proposed scheme would capture many sites that should not be covered by a cyber bullying scheme, such as ordinary websites with comment and chat features.
- The standard for “harm” is vague and inconsistent, and would be difficult to apply.
- The proposed scheme is not flexible enough to respond to rapid changes in technology and consumer activity. A cooperative approach would be much better placed to adapt to changing technologies and provide a faster response, at scale.
- There is no due process built into the proposed scheme for those who wish to challenge a complaint.

There is no demonstrated need for new cyber bullying offences

Leading experts agree that existing laws are sufficient to tackle the crime of cyber bullying. The problem, according to these experts, is not that the laws do not exist, but rather that there is a general lack of awareness of the existing criminal and civil laws that are available. This problem could be addressed by an e-safety commissioner. A commissioner would have the chance to see how they could best work with government agencies, NGO and industry groups to address cyber bullying and promote broader cyber safety initiatives. The new commissioner would be able to properly identify whether social media sites are taking appropriate steps to make sure their users have proper and effective tools to flag content, and which companies and organisations are not being cooperative. The commissioner could also be tasked with reviewing the effectiveness of the Government’s cyber bullying initiatives with a view to considering what could assist victims of cyber bullying more fully.

At odds with the Government’s deregulation agenda

As outlined, there are existing laws and processes to address cyber bullying. In light of this, and the fact that legislated mandatory removals would be highly problematic, Google submits that a case has not been made out for further government regulation, and that the legislated mandatory removals scheme outlined in the Discussion Paper would be at odds with the Government’s deregulation agenda.

SUBMISSION

Introduction

Google is pleased to have this opportunity to comment on the Government's Discussion Paper on Enhancing Online Safety for Children. We welcome this initiative by the Government to engage with industry and other stakeholders to consider best practice measures for protecting children online, and we look forward to working with the Government on this important consultation.

Google shares the Government's objective of keeping children safe online. This objective requires ongoing effort. We agree that mechanisms for handling content and cyber bullying concerns quickly are essential, and that children must be able to access assistance with online safety concerns.

Google submits that the key challenge in addressing cyber bullying is ensuring that the community is educated to understand that cyber bullying is against the law, and to know what to do if cyber bullying occurs. There are already well-functioning laws and industry processes in place to tackle cyber bullying in Australia.

1. Industry sets global best practices to address online safety

There is a great deal being done by social media sites and other stakeholders to address online safety and particularly cyber bullying. The major social media sites used by young people in Australia have highly developed and effective systems and policies in place to address cyber bullying, and work cooperatively with Government, NGOs and caregivers to enhance online safety for children.

Social media sites have strong commercial incentives to build a positive and safe online community. Providers want their brand associated with a good user experience, where users are comfortable, safe and secure.

Australia has a healthy and promising digital economy, which is set to provide further growth and opportunity. The internet contributed $50 billion directly to the economy in 2010 and even more in other benefits for households and business[3]. It is also important to keep in mind that there are tremendous benefits of online social networking. Research from the Young and Well CRC (YAW-CRC) has found that "there are a number of significant benefits associated with the use of social networking services (SNS) including: delivering educational outcomes; facilitating supportive relationships; identity formation; and, promoting a sense of belonging and self-esteem. Furthermore, the strong sense of community and belonging fostered by SNS has

[3] Deloitte *Connected Continent*, 2010 http://www.deloitte.com/view/en_AU/au/services/financial-advisory/transaction-group/17a9ba2c5d381310VgnVCM1000001a56f00aRCRD.htm

the potential to promote resilience, which helps young people to successfully adapt to change and stressful events." (http://www.inspire.org.au/wp-content/uploads/2011/04/FAQ_CRC1.pdf)

In order to participate fully in the digital economy, Australians need to be equipped and empowered to be capable digital citizens. Being a capable digital citizen includes having the necessary skills be to be smart, safe and responsible online. It includes understanding the rights and responsibilities that come with online interactions. Capable digital citizens have the skills and knowledge to take advantage of the opportunities of the online world while minimising the risks.

Part of encouraging Australians to be good digital citizens is making it clear that harassing and bullying behaviour - online or offline - is never OK. It also includes encouraging them to use processes and mechanisms that are in place to enable a responsive approach where bullying does occur. The industry, government and the community need to work together to get Australian youth to be upstanders, not bystanders to acts of bullying online and offline. To do this they need to be leaders, to know the tools available to them, and to know who to go to if help is needed.

1.1 Google's approach to cyber safety

Google promotes online safety through a combination of:

- **Policies** - We have strong policies and guidelines in place that set out acceptable content and conduct. Users are warned that postings that breach these policies and guidelines will be removed, and that they may be permanently banned from using the site.
- **Tools** - We have tools in place (such as Google SafeSearch, and Safety Mode for YouTube) that empower people to manage their online experience. We also provide simple and effective ways for users, including young people, to register complaints about inappropriate content or conduct. Industry leading tools such as the YouTube flag system enable users to report content that violates our policies. We respond quickly to these complaints: we have processes for reviewing complaints from users and other parties - 24 hours a day, seven days a week - and we rapidly remove content that is found to be in breach of site guidelines/policies.
- **Education** - We provide educational resources such as the Google 'Safety Centre' website (www.google.com.au/safetycenter/) and the YouTube Safety Centre (www.youtube.com/yt/policyandsafety/) to offer advice on how to use Google products in a smart, safe and responsible way. Our product Help Centres provide our users with tips and articles for managing their experience while using Google products and staying safe online.
- **Partnerships** - We partner with NGOs to educate families about cyber safety and develop anti-bullying resources. We invest a large amount of funding, time and other resources on cyber safety initiatives.
- **Cooperation** - We cooperate with governments and law enforcement agencies to address cyber bullying. We are a signatory to the Cooperative Framework on Complaints Handling for Social Media that is in place with the Australian government.

Strong policies prohibit use of Google services for harassment and bullying

Harassing and bullying behaviour is not acceptable when using Google's services. e.g:

- The YouTube Community Guidelines warn users that "predatory behaviour, stalking, threats, harassment, invading privacy, or the revealing of other members' personal information" is prohibited, and that anyone caught doing these things may be permanently banned from YouTube.
- YouTube's Harassment and Cyber bullying policy warns that YouTube will remove "comments, videos or posts where the main aim is to maliciously harass or attack another user".
- The Google Safety Centre provides information for families on Google tools that are available to help them keep their children safe online.

Providing a means for victims of cyber bullying to register a complaint

Of course, it's not enough to have policies prohibiting inappropriate content; responsible social media sites also provide a simple mechanism for victims of cyber bullying to register a complaint regarding particular content that breaches the site guidelines/policies. For example YouTube users can flag content that breaches the YouTube Community Guidelines. Flagged content is reviewed, and content that is found to violate the guidelines is removed.

Google has in place processes for reviewing complaints from users and other parties - 24 hours a day, seven days a week. We quickly take action on these complaints, removing content that is found to be in breach of site guidelines/policies.

A case study - The YouTube flag system

People upload over 100 hours of video to YouTube every minute. With so much content on the site, it would be impossible to review it all. That's why we empower the YouTube community to flag content that they find inappropriate.

Users have the power, through our industry-leading tools, to report content that they think violates our policies. For instance, if a YouTube user thinks a video violates our Community Guidelines, they can click a button to flag it for review. Our dedicated teams manually review these flagged videos 24 hours a day, 7 days a week. They look to determine whether the video violates our policies, examining not only the content of the video but its context and intent. When our teams encounter a video that violates the Community Guidelines, we remove it quickly. Videos are also removed in response to legal complaints, including valid court orders issued against the person who posted the video.

In addition, You Tube users are able to manage the type of content available to them by opting in to "Safety Mode" which can help screen out potentially objectionable content.

Empowering people with tools to manage their online experience

Across its services, Google provides tools to enable people to manage their online experience.

Google provides the Google SafeSearch tool which uses advanced technology to block pornographic and explicit content from search results. Users can customise their SafeSearch settings by searching for 'Google SafeSearch' and following the prompts.

We also provide Safety Mode for YouTube. This is an opt-in setting that helps screen out potentially objectionable content that a user may prefer not to see or don't want others in their family to stumble across while enjoying YouTube. An example of this type of content might be a newsworthy video that contains graphic violence such as a political protest or war coverage. Users can customise their SafeSearch settings by searching for 'YouTube Safety Mode'. Safety Mode can be switched on from the bottom of any YouTube page.

Importantly in the context of cyber bullying, the available tools include the ability for individuals to block others from interacting with them, to post content privately and to choose to pre-moderate comments or disallow commenting on their uploads altogether.

Educating people about how to stay safe and secure online

A central plank in any approach to cyber safety is to ensure that Australians - and young people in particular - understand the issues they may face online and the tools that are available to help them manage their experience.

Google provides educational resources, such as the Google 'Safety Centre' website www.google.com.au/safetycenter) and the YouTube Safety Centre (linked to at the bottom of each YouTube page) to offer advice on how to use Google products in a smart, safe and responsible way.

Also through our product Help Centres, we provide our users with tips and articles for managing their experience while using Google products. We also invite our users to tell us about illegal content or abuse they encounter on the web or in our products through our Help Centres.

1.2 Google works with NGOs and other stakeholders to raise cyber safety awareness

Google works with Australian child safety and wellbeing organisations to educate people about cyber safety. For example:

- For a number of years now Google has supported education and children's help programs run by NAPCAN, Kids Helpline, Bravehearts, the Young and Well CRC and

The Alannah and Madeline Foundation.

- We work with groups like The Alannah and Madeline Foundation to promote e-Safety in schools. We recently granted funding for 100 new schools to be signed up to their eSmart schools program in NSW.[4]

- We worked with Smart Online, Safe Offline (SOSO) on the launch on YouTube of an interactive cyber bullying campaign, called Cyber Bullying Affects Real Lives. [5] Madelene McGrath, NAPCAN's SOSO Project Manager, has said that "Google and YouTube's support for this campaign was invaluable, and by working closely with YouTube to become part of the fabric of the site, we were able to engage far more effectively with our youth audience and deliver our message in a highly impactful way. Google and YouTube went well beyond being a media publisher and acted as a strategic partner throughout, ensuring the delivery of a highly successful campaign."

- Google partnered with The Alannah and Madeline Foundation to support a wide ranging 'Good to Know' campaign to educate parents, teachers and kids about staying safe online.

- We work with Bravehearts to promote child safety and keep children safe from harm online. We take advice from organisations like Bravehearts[6] especially when updating our policies to combat child sexual assault and our work to better understand the ever-changing landscape of offender behaviour and language.

- We are actively involved in promoting Safer Internet Day,[7] which promotes safer and more responsible use of online technology and mobile phones, especially amongst children and young people, across the world. The following screenshot shows the Google

[4] http://www.amf.org.au/Assets/Files/MR_eSmart_new.pdf
[5] www.youtube.com.au/soso
[6] http://google-au.blogspot.com.au/2014/02/guest-post-from-bravehearts-protecting.html
[7] http://www.saferinternetday.org/web/guest

homepage on Safer Internet Day this year:

The link directed users to the Google Safety Centre[8]. See also a recent Google blog posting[9] on safety initiatives associated with Safer Internet Day. Advice from our partners like The Alannah and Madeline Foundation and Kids Help Line is an integral part of our "For Families"[10] section of the safety centre.

1.3 Google works cooperatively with government and law enforcement

Google works cooperatively with government and law enforcement bodies.

We have a legal team devoted to interactions with law enforcement 24 hours a day, 7 days a week. We respond, quickly and at scale, to thousands of law enforcement requests for assistance, and hundreds of subpoenas, each year. We also cooperate with the police and the ACMA to disseminate educational material.

We have developed an industry wide online safety tips brochure,[11] designed to help schools and MPs get information to parents and children. The brochures have been sent to MP offices, many of whom requested further copies. The online version of the brochure was also promoted by the ACMA.

Google is an active participant in the Consultative Working Group on Cyber Safety, which, in

[8] http://www.google.com.au/safetycenter/families/start/
[9] http://googleasiapacific.blogspot.com.au/2014/02/safer-internet-day-helping-families.html
[10] http://www.google.com.au/safetycenter/families/manage/bully/
[11] http://www.aimia.com.au/enews/Industry%20Development/Digital%20Policy%20Group/AIMIA%20Digital%20Policy%20Group%20Keeing%20Australians%20Safe%20Online%20Public.pdf

cooperation with the Department of Communications, produced the Cyber safety Resources website.[12]

We are also a signatory to the Cooperative Framework for Complaints Handling on Social Media.[13] Under this framework, Google, along with other major social networking services, has undertaken voluntarily to:

- Have in place policies for acceptable use and provide clear information about what constitutes inappropriate behaviour on the sites as well as the consequences of breaching the acceptable use policy.
- Have mechanisms for reporting inappropriate content, contact or behaviour as outlined in the policies for acceptable use, and enable users to have access to information they need to make an effective report.
- Have in place a process for reviewing and acting on complaints promptly.
- Have a contact person/s with whom the Government can discuss issues and any appropriate messaging to the community and media in response to issues as they arise.
- Encourage users to understand the functionality on their sites, including reporting tools, and to provide clear guidance designed to give people the tools, knowledge and skills to navigate their services safely.
- Take steps to help users be aware of the importance of being smart, safe and responsible online.
- Contribute to, support and collaborate with the Australian Government, as appropriate, on relevant cyber safety initiatives.
- Innovate to provide useful services that promote user safety.
- Provide information on how they give effect to this cooperative arrangement.
- Meet with government officials on a bilateral basis every six months to discuss trends and emerging issues.
- Provide the Government's Online Safety Consultative Working Group with information on trends and emerging issues every twelve months.

Google has met and will continue to meet the obligations it has undertaken as part of the Cooperative Framework.

2. Existing laws adequately deal with cyber bullying

The discussion paper suggests that there are "inadequate remedies" available when children are the victims of harmful, aggressive or bullying material targeted at them using the internet. Google submits that this is not the case.

---

[12] http://www.cybersafety.communications.gov.au/resources

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

2.1 Existing laws that apply to cyber bullying

Criminal legislation at the State and Territory level already allows for the prosecution of harassing threatening and intimidatory behaviour through a combination of assault, threatening and stalking offences. In addition to legislation in their own jurisdictions, State and Territory law enforcement agencies can rely on the offences found in the Criminal Code which, in conjunction with civil remedies, directly address these forms of behaviour.[14] **Annexure A** to this submission is a table that sets out in detail the range of legal remedies that are potentially available to victims of cyber bullying, but in summary these include:

- Commonwealth laws that make it a crime to use the internet or a phone in a threatening, harassing or offensive way
- Commonwealth and state/territory laws that prohibit threats and intimidation
- State and territory anti-stalking laws
- Emerging case law dealing misuse of private/personal information
- Defamation law

2.2 Existing laws sufficiently cover cyber bullying

Australia already has in place existing criminal and civil laws in all jurisdictions that apply to cyber bullying activities. This provides a broad range of legal approaches and remedies to appropriately address cyber bullying behaviour. Given that existing laws adequately cover cyber bullying activities, it is questionable whether adding a new cyber bullying provision would provide victims of cyber bullying with any additional legal remedies. For example, a recent report on NSW and Commonwealth laws that are relevant to cyber bullying - *New Voices/New Laws* - the National Children's and Youth Law Centre (**NCYLC**) contains a detailed survey of the wide range of State and Commonwealth laws that are available to address cyber bullying behaviours in NSW. The NCYLC's Lawstuff website [15] also provides information on the laws that apply in other states and territories.

Similarly, the Joint Select Committee on Cyber-Safety[16] heard evidence to the effect that existing laws are capable of providing a remedy for cyber bullying. In its 2011 report, the Committee referred to the following evidence from relevant experts:

> *Professor Marilyn Campbell [School of Learning and Professional Studies, Queensland University of Technology] expressed the view that:*

[14] Submission by the Attorney General's Department to the Joint Select Committee on Cyber Safety
[15] http://www.lawstuff.org.au/

[16] http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=jscc/report.htm

> *Even though there are not so-called specific anti-cyberbullying laws, there are* ***enough criminal justice laws on cyberstalking, harassment and telecommunications that, if you wanted to criminalise a child's behaviour, the laws are there****—except that, as you know, children under 10 are not held criminally responsible for their actions no matter what they do. Between 11 and 14, it is up to the court to decide whether they intended to commit a criminal act. So it is not about knowing it was naughty and knowing it was wrong and responding to something and not thinking before they clicked. It is about whether they intended to commit a criminal act and whether they then went ahead realising that it was a criminal act.*[17] (emphasis added)

The Committee heard similar evidence from the Attorney-General's Department:

> *The Attorney-General's Department also noted that criminal legislation at State/Territory level allows for the prosecution of harassing, threatening and intimidatory behaviour through a combination of assault, threatening and stalking offences. These jurisdictions can also rely on offences in the Commonwealth Criminal Code which directly address these abuses.* [18]

2.3 Lack of awareness of existing cyber bullying laws

Google believes that there is much work to be done to raise the level of awareness regarding the existing remedies. A common theme in the submissions received by the Joint Select Committee on Cyber-Safety from NGOs and others regarding cyber bullying laws is that young people and their parents are not aware of the legal remedies that are available to respond to cyber bullying:

- The Association of Independent Schools of South Australia called for a promotional campaign to inform school communities what constitutes an e-crime.The Association said that *"many students may not be aware that what they are doing is not only bullying, but it may also be against the law*."[19]
- Similarly, the Office of Youth submitted that "*people do not know what is legal and what is not".* [20]
- Professor Phillip Slee from the Australian University Cyberbullying Research Alliance informed the Committee that young people were not aware that uploading images or taking images could constitute stalking. He urged greater education for the community around what constitutes criminal activity. [21]
- The Stride Foundation submitted that interviews with cyber bullies have often revealed they considered their online harassing behaviour as 'pranking' or joking around. The

[17] paras 11.62 to 11.63
[18] para 11.64
[19] High-Wire Act: Cyber-Safety and the Young para 11.99
[20] Ibid para 11.100
[21] Ibid para 11.100

Foundation said that both students and adults involved with online behaviour needed to understand that "*the sending of offensive or harassing messages is considered by the law as assault*". [22]

Far from needing new laws to address cyber bullying, what appears to be needed is a more effective way of educating young people, teachers and parents regarding the legal status of this conduct. Cyber bullies need to be made aware that they could be breaking existing laws, and victims need to know that there are legal remedies (as well as self-help remedies such as those provided by social networking services) available to them if they are being bullied.

Raising awareness has been shown to be effective

Simply raising awareness of the legal consequences of cyber bullying has been shown to be effective in changing behaviour. The NCYLC provides youth-friendly advice on the NSW and Commonwealth laws that apply to young people's online behaviour, including via a prezi, and recently reported that this awareness raising had actually changed behaviour":

> *.. the prezi has a real effect on young people's behaviour and attitudes, with **68.3% of students saying 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 feel more confident about being able to deal with these issues.*[23] (emphasis added)

3. Google supports better coordination of cyber safety initiatives

Google believes there is value in having a central point of contact and coordination, such as an e-safety commissioner. Centralisation could play an important role in:

- **Coordinating** existing cyber safety resources and initiatives
- **Educating** the community and law enforcement bodies about cyber bullying including the complaint and removal mechanisms already in place and the nature of Australia's existing laws against cyber bullying
- **Cooperating** with industry to quickly resolve cases of cyber bullying, building on the existing cooperative framework. A commissioner would be well placed to exert influence - where required - and liaise with Government, police, members of the public, and online providers to ensure that the Government's objectives are met.

[22] Ibid para 12.6
[23] http://prezi.com/jiudkskuct0h/new-voicesnew-laws-report/

The Discussion Paper seeks comment on the most appropriate means of establishing a new e-safety commissioner, as well as on the tasks that the commissioner could perform.

3.1 Appointing an e-safety commissioner

As the Government has noted[24], best practice principles for establishing a new government position as outlined in the *Governance Arrangements for Australian Government Bodies*[25] require that there be no unnecessary proliferation of government bodies, and that a new function, activity or power should be conferred on an existing body unless there is a persuasive case to form a new body.

In Google's submission, adherence to these best practice principles would be best achieved by adopting either Option 3 (appointing an Associate Member of the ACMA as commissioner) or Option 4 (an NGO with expertise in cyber safety).

3.2 The role of an e-safety commissioner

Google supports the creation of a central point of contact and coordination, such as an e-safety commissioner (an Associate Member of the ACMA board or an NGO), who is an accessible and central point of contact for the public and industry on matters relating to cyber bullying.

Coordinating existing cyber safety resources and initiatives

An e-safety commissioner could be a point of contact for a young person, parent or teacher who was unsure what remedies or resources were available to address cyber bullying.

The commissioner could undertake an audit, or "stocktake", of existing educational resources and programs with a view to advising the Government what, if anything, is needed in the way of supplementing existing programs or streamlining or augmenting existing resources. We see this as an important role - identifying areas of duplication and gaps, and creating a cohesive whole of government strategy for these programs would have a significant impact.

Educating the community and law enforcement bodies about existing remedies

An e-safety commissioner could actively promote awareness of existing laws and resources and provide a central resource for cyber safety information for Australian parents and children and the wider community.

---

[24] Discussion Paper p 6

[25] Governance Arrangements for Australian Government Bodies, Australian Government Department of Finance, August 2005

Cooperating with industry to quickly resolve cases of cyber bullying, building on the existing cooperative framework.

The e-safety commissioner could act as a 'go-to' person for parents or young people who considered that their complaints were not being adequately addressed by social media services. It is likely that a commissioner would develop a productive relationship with industry and therefore be well placed to work cooperatively with providers to ensure that they continue to meet best practice in responding swiftly to cyber bullying concerns. Of course, a commissioner would also be well placed to identify those services or platforms - if any - that fail to do this, and to advise the Government of this.

4. Concerns with legislating mandatory removals

Google has a number of concerns with legislating mandatory removals:

- There is no evidence provided to suggest that a formal legislative process would work better than cooperative industry processes.
- The proposed scheme would not capture many social media sites, including many popular social messaging apps that are popular with teenagers. Public expectations regarding the ability of a legislated removals scheme to address cyber bullying are likely to greatly exceed the reality of what such a scheme is capable of achieving.
- The proposed scheme would capture many sites that should not be covered by a cyber bullying scheme, such as ordinary websites with comment and chat features.
- The standard for "harm" is vague and inconsistent, and would be difficult to apply.
- The proposed scheme is not flexible enough to respond to rapid changes in technology and consumer activity. A cooperative approach would be much better placed to adapt to changing technologies and provide a faster response, at scale.
- There is no due process built into the proposed scheme for those who wish to challenge a complaint.

4.1 No evidence provided to suggest that a legislative process would work better

The obligations that the Government would seek to impose legislatively are already covered by the Cooperative Framework for Complaints Handling on Social Media,[26] which we have discussed above. There is no evidence that we are aware of that this voluntary framework is not being met by the services that would be covered by the proposed legislated removal regime. In fact Google has not received any requests from Government under the scheme since its implementation. This exemplifies why legislation is not needed.

---

26 http://www.communications.gov.au/__data/assets/pdf_file/0004/160942/Cooperative_Arrangement_for_Complaints_Handling_on_Social_Networking_Sites.pdf

4.2 The proposed scheme would only apply to services that already have policies and processes in place to address cyber bullying

It is significant, in our view, that the legislated removals scheme outlined in the Discussion Paper would have no impact on many smaller social media services that are commonly used by young people.

One reason that these smaller services would appear to fall outside of the proposed regime is their size: the Discussion Paper says that the regime would apply to "large" social media sites, with "large" being defined according to "objective criteria such as the number of user accounts held with the site by Australians". [27] This is despite the fact that it is the large social media sites that are already meeting global best practice and actively engaging with parents and children, government, NGOs and other stakeholders to address cyber bullying.

The fragmented social media messaging apps ecosystem - and the speed with which new apps enter the market and capture user engagement - will be difficult for any Government agency to keep up with e.g. snapchat has grown in just under 3 years to its current size and popularity. Official distinctions between "large" and "small" social media sites are likely to lag behind their real-time growth rate and end up making the regime's classifications obsolete.

Another reason that some services would fall outside of the proposed regime is that the definition of "social media site" would appear not to capture services that are not "web based". The Discussion Paper refers to two definitions of "social networking sites"; the 'Boyd and Ellison' definition, and the Office of the Australian Information Commissioner (OAIC) definition. Both of these definitions appear to apply only to web-based sites and services. Notwithstanding that messaging apps use a phone or tablet's data plan to send messages, this is not generally understood to be use of the 'world wide web'. This would take them outside the scope of the Government's proposed cyber bullying reforms.

4.3 The proposed scheme would be overbroad in ways that do not appear to be intended

Google is also concerned that the scheme outlined in the Discussion Paper would have an overbroad operation in ways that do not appear to be intended. An extremely wide range of websites could be captured by the proposed scheme.

The Discussion Paper asks whether two existing definitions of "social networking sites" are

[27] Discussion Paper, p 12

suitable for the purposes of the proposed scheme - the 'Boyd and Ellison' definition, and the Office of the Australian Information Commission (OAIC) definition. Boyd and Ellison refer to "web-based services", and the OAIC refers to "websites".

The trend of social media integration in website design and consumer engagement means that a very large number of websites that do not appear to be intended by the Government to come within the proposed scheme would in fact be captured, and as a result, subject to a legislated take-down regime. Consider the following examples, which are merely reflective of the trend *today*:

- NineWest is integrating customer's Pinterest and Twitter experience on its own website[28]
- Nike 6.0 is integrating social media on its website and creating a space - the Nike community - to engage on the website rather than on disparate social media platforms[29].
- Sporting bodies are increasingly integrating social media into event websites. For example, Tennis Australia's 2014 Australian Open website had a 'Social Leaderboard' feature, compiling discussions and content from various social media platforms.[30]
- Real estate agents are also integrating property related information with social media functionality to be used by agents as well as consumers. For example, Housenet.com.au [31] and the Real Estate Social Network.[32]

Over time, the range of players to which the proposed scheme would apply is considerable. These examples highlight the difficulties of a legislated scheme as opposed to more nuanced, collaborative responses to cyber safety.

4.4 The standard for "harm" is vague and inconsistent

The proposed scheme would apply to any material the Commissioner deemed to be 'harmful'. The Discussion Paper describes the proposed standard in the following ways:

- "material that is harmful to a child" p 5
- "harmful, aggressive and bullying material" p 9
- "...the material would be likely to cause harm or distress to the child" p 15
- "material which is potentially harmful or distressing to a child" p 19
- "serious emotional distress" p 24

Google is concerned that the standard for harm as set out in the Discussion Paper is vague and inconsistent. The following examples illustrate some of the difficulties in applying this standard:

[28] http://www.postano.com/blog/nine-west-case-study
[29] See How to Integrate Social Media Content into Your Website
[30] http://www-03.ibm.com/press/au/en/pressrelease/42932.wss
[31] http://www.housenet.com.au/
[32] http://www.resaas.com/

Case Study - Western Force 'quokka incident'

An incident involving alleged mistreatment of quokkas occurred at a Western Force rugby team pre-season trip to Rottnest Island. One member of the team, James O'Connor, was at the time 17 years old.

Some social media commentary in relation to the team incident referred to players being involved in "an off season Quokka disgrace" or players being involved in "drunken antics on Rottnest Island". Social media comments about the broader performance of the team that year included comments about James O'Connor such as "little snothead" and "I hope [another team] break both his legs. In several places".

Would a social media site be required to assess whether comments about James O'Connor could be objectively harmful to a child, or whether James O'Connor's individual personal characteristics were relevant?

Case study - Nikki Webster at the Sydney 2000 Olympics

Nikki Webster was 13 at the time she performed at the opening ceremony of the Sydney Olympics. She was subsequently parodied, made the brunt of jokes, and even had her effigy blown up on a popular television show. In her own words, she describes the media attention as hurtful, bullying and inappropriate, which translated to real world bullying at school.

How would a site be expected to assess whether commentary of this kind on its platforms in relation to a child was harmful?

4.5 Not flexible enough to respond to rapid changes in technology and consumer practice

A legislative regime is likely to be insufficiently flexible to respond to rapidly changing technological developments, as well as constantly shifting consumer practice. For this reason, public expectations regarding the ability of a legislated removals scheme to address cyber bullying are likely to greatly exceed the reality of what such a scheme is capable of achieving. A cooperative approach with industry is much better placed to respond flexibly, quickly and at scale to changes in technology and consumer practice.

4.6 No due process built into the scheme

There does not appear to be any provision for due process in the proposed scheme. For example, what process should apply if the proposed scheme is abused (eg by individuals making vexatious complaints and/or seeking removal of legitimate content)? Our experience with

notice and takedown in the copyright context has shown not only that mandatory takedown schemes can be abused, but also that there will often be scope for legitimate disagreement as to whether or not content that is the subject of takedown notice should in fact be removed.

5. Inconsistent with the Government's deregulation agenda

The Government's stated policy[33] is to impose regulation only where "it is absolutely necessary and [where] no sensible alternatives [are] available".

Also the Office of Best Practice Regulation handbook, published by the Office of Regulation Review (ORR), sets out the best practice process for policy design and evaluating between competing regulatory approaches. This requires consideration of at least the following questions:

- Has a case for regulation been made out?
- Is this purpose already being achieved without regulation? (by user-regulation, industry self-regulation, market-based mechanisms etc)? If so, is the best approach to "take no action"?
- If not, how can the purpose be achieved with the least amount of government intervention; i.e. what policy levers apart from government regulation are available to achieve the desired policy outcomes?
- Are there any technical or other obstacles that make it likely that a particular mode of regulation is likely to be ineffective, thus imposing costs on industry with no public benefit?

Google submits that applying the ORR principles to the matters raised in this submission suggests that at this time a case has not been made out for further government regulation, and that better collaboration, coordination and education in the context of the existing laws and processes is the most effective approach to dealing with cyber bullying in the current environment. In particular, we note that the obligations that the Government would seek to impose legislatively are already covered by the Cooperative Framework for Complaints Handling on Social Media which we have discussed above, and that there is no evidence that we are aware of that this voluntary framework is not being met by the signatory services.

Google is grateful for the opportunity to present our views on the proposals in the Discussion Paper. We look forward to continuing this important discussion.

Ishtar Vij
Public Policy and Government Affairs
Google Australia

[33] http://www.joshfrydenberg.com.au/guest/SpeechesDetails.aspx?id=225

Annexure A

Existing laws that apply to cyberbullying

1. Criminal remedies

Relevant law	Comment
***Criminal Code Act 1995* (Cth) (CCA)** *:* s 474.15 CCA - offence for a person to use a carriage service to threaten to kill or to cause serious harm to another person or to a third person while intending the target to fear that the threat will be carried out. s 474.16 CCA - offence for a person to use a carriage service to send a hoax communication intending to induce a false belief that an explosive, or a dangerous or harmful substance or thing, has been or will be left somewhere. s 474.17 CCA - offence to use a carriage service to menace, harass or cause offence. s 474.22 CCA - offence to use a carriage service for child abuse material (eg images of sexual assault)	Each of these CCA offences would apply to communications via text, social media pages etc The DP notes that since coming into effect in 2005, s 474.17 of the CCA has been used to support 308 successful prosecutions for a broad range of conduct involving the internet, "including eight prosecutions involving defendants under 18 years of age". [34]
Stalking laws Each state and territory has anti-stalking legislation: *Crimes Act 1900* (ACT) s 35 Crimes Act 1900 (NSW) s 545B	Western Australia is the only state that has not made *specific* provision for cyberstalking in its anti-stalking provisions. See this report of a cyberstalking prosecution in Victoria in 2010.

[34] DP, p 21

Criminal Code 1983 (NT) s 189 *Criminal Code 1899 (Qld) s 359A* Criminal Law Consolidation Act 1935 (SA) s 19AA Criminal Code Act 1924 (Tas) ss 192, 192A Crimes Act 1958 (Vic) s 21A Criminal Code 1913 (WA) ss 338D, 338E	
Criminal Assault While some states expressly or implicitly provide that words or images will *not* suffice for criminal assault, it appears that this remedy is available in other states for threats etc conveyed via text, social media etc. See in particular s 20 of the *Criminal Law Consolidation Act 1935* (SA) ('threatens by words or conduct') and s 187 (b) of the *Criminal Code 1983* (NT) (threat may be 'evidenced by bodily movement or threatening words)'.	
Assault at school - NSW The NSW Crimes Act contains a specific provision - s 60E - dealing with assault, stalking, harassment or intimidation of any school staff or student while attending the school.	
Threats Each state and territory has provisions making it an offence to make threats that cause a person to fear physical violence: *Crimes Act 1900* (NSW) s 31 - an offence to send any document threatening to kill or cause bodily harm *Criminal Code 1899* (Qld) s 308 *Criminal Code Act 1924* (Tas) s 163 *Crimes Act 1900* (ACT) s 30 *Criminal Code 1983* (NT) s 166	

Criminal Law Consolidation Act (SA) ss 19(1)-(3) *Crimes Act 1958* (Vic) s 20 *Criminal Code 1913* (WA) ss 338A-B.	
Torture Commentators[35] have suggested that laws prohibiting torture may have potential application to cyberbullying: s 320A of *Criminal Code 1899* (Qld) makes it an offence to torture another person. Torture is defined as "the intentional infliction of severe pain or suffering on a person by an act or series of acts done on 1 or more than 1 occasion", and for the purposes of the provision, pain or suffering "includes physical, mental, psychological or emotional pain or suffering, whether temporary or permanent".	

2. Civil remedies

Relevant law	Comment
Privacy Some states have recognised a common law cause of action for breach of privacy that has potential application to cyberbullying: Queensland - Gross v Grosse v Purvis - a victim or criminal stalking was entitled to damages for breach of privacy arising from the stalking on the basis that the stalker had intruded upon her privacy in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities and which caused her detriment in the form of mental physiological or emotional harm or distress. The reasoning in this case would apply equally to cyberstalking.	

[35] Kift, Campbell and Butler, *Cyberbullying in Social Networking Sites and Blogs: Legal Issues for Young People and Schools* [2010] JILawInfoSci 13

See also Jane Doe v ABC (Victorian County Court judge found that a media disclosure of private details warranted damages for breach of privacy).	
Tort of defamation Each state and territory has a Defamation Act that provides for damages for defamatory publications. Content that exposes a person to severe ridicule (ie a posting on a social media page that is able to be accessed not only by the victim but by other people as well) is capable of being defamatory. A one-on-one text would not suffice.	
Tort of assault Threats of violence transmitted via text, social media etc may be actionable as civil assault, provided that the victim could prove that he/she had been made to apprehend immediate physical violence.	