ISSUE DATE: 7 MARCH 2014

TELSTRA CORPORATION LIMITED SUBMISSION TO THE AUSTRALIAN GOVERNMENT'S DISCUSSION PAPER ON ENHANCING ONLINE SAFETY FOR CHILDREN

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Telstra welcomes the opportunity to provide this submission in response to the Australian Government's Discussion Paper on *Enhancing Online Safety for Children.*

Advances in technology are transforming the way Australians connect with friends, family and the broader community. At Telstra we strive every day to deliver our customers access to the best products and services possible so they can maximise the benefits of new communication technologies. At the same time, we are committed to offering products that are safe and secure, especially for vulnerable members of the community.

We share the Government's goal of improving the online safety of children and young people. Cyber safety and, more specifically, cyberbullying are important public policy issues for all Australians. As Australia's largest internet and mobile phone service provider, Telstra plays a leading role in promoting cyber safety.

Our leadership role includes supporting a wide range of consumer education programs, ensuring our networks are robust and secure, funding research, partnering with like-minded organisations, assisting both government and industry to draft policy and codes, and participating in global initiatives. We also provide our customers with relevant information, expertise, tools, products and services so that they are better equipped to exercise reasonable care and responsibility to achieve the best value from their digital and online experiences and do so in a way that does not limit the range of legitimate and positive uses of the internet.

Telstra advocates that addressing cyber safety is a responsibility that is shared between many different bodies, including government, law enforcement, non-profit organisations, industry, schools, parents and children. In a 'culture of responsibility'[1], through a co-ordinated effort, each group plays a role, to help keep children safe from harm, build digital resiliency and help grow responsible digital citizens. It is important that all groups work together to achieve a safe digital and online future for all Australians.

In respect of the issues and questions raised in the Government's Discussion Paper, it is Telstra's view that:

[1] Family Online Safety Institute, 'Broadband Responsibility: A Blueprint for Safe & Responsible Online Use', 2010

- Smart, ethical and socially aware digital experiences require individuals to adopt responsible and respectful online behaviours. The best way to achieve this is through education.
- In seeking to improve cyber safety outcomes, the Government should target any new obligations on the platform or site where bullying or offensive material exists, rather than the underlying internet service or relevant carriage service provider.
- We believe the Government's policy objectives can be realised without creating any new obligations on service providers to retain data, investigate users or block access to sites. Internet and carriage service providers already operate under a host of legislative arrangements, including the Telecommunications Act, Privacy Act and the Telecommunications (Interception and Access) Act, that create obligations to protect customer information and provide reasonable assistance to government agencies in relation to areas such as cyber crime. Consistent with the Government's red tape reduction agenda, any policy reform in the area of cyberbullying needs to be carefully designed so to not replicate, conflict with or cause confusion around these existing obligations.
- From a technical perspective, if Telstra were asked to investigate an incident, it is unlikely we could readily identify an individual operating within a social media site. Telstra's systems are not configured to enable such a level of scrutiny of our customers' online activities. Also feedback from our customers suggests many would not welcome this degree of oversight by a service provider. As such, service providers are unlikely to be in a position where they could efficiently and effectively, for example, ensure that a request for a social media site to takedown an accountholder, posting or otherwise is enacted.
- Consistent with best practice regulatory principles, a cost-benefit analysis should take place prior to any legislative change.
- The Government could consider the merits of the development of a standard industry approach, such as a registered code of conduct or co-operative arrangement, to address the process of complaints handling on social networking sites. Examples of such codes include: the European Union's Better Internet for Kids that has the involvement of a coalition of CEOs of all major technology companies; and the Communications Alliance Handling of Life Threatening and Unwelcome Communications Code (C525:2010).

INTRODUCTION

Social media offers a range of benefits to all ages including the ability to form and maintain friendships, and the creation and sharing of content and ideas. Social media is an integral part of the shift towards using information communication technology for social purposes and it is rapidly becoming integral to the conduct of business. Popular social media activities for children include playing games, posting their own updates, posting comments or photos on someone else's posts as well as private messaging.[2] Although social networking presents social benefits, it also exposes users to increased risks.

A recent Telstra survey[3] into the prevalence of cyberbullying found that 52 per cent of 18–25 year-olds reported at least some exposure to cyberbullying: with 10 per cent admitting to participation (bullying), 24 per cent identifying as the victim and 43 per cent having witnessed cyberbullying. Overlap among the involvement types is high, particularly among those who self-identified as a 'bully'; 71 per cent have been victims themselves, and 81 per cent have been witnesses. Cyberbullying can have serious negative impacts on a young person's wellbeing, leading in some cases to sleep loss, emotional distress, low self-esteem, and can be a trigger for suicidal ideation.[4] Research suggests a strong correlation between being bullied offline and being cyberbullied. As a 2009 independent report noted, research showed that 'some of the most troublesome risks are strongly associated with offline risks and that these two worlds do not exist independently. Thus, in order to address online risks, it is crucial that offline behaviours are also considered.'[5]

As an organisation that takes its corporate responsibilities seriously, Telstra supports, and has developed, a number of cyber safety initiatives for children, young people, parents and schools. These include the creation and distribution of consumer education resources and face-to-face workshops, educational programs carried out in partnership with government and the not-for-profit sector, participation in industry bodies, clear social media protocols, the provision of a range of parental control products and the participation in Interpol's 'worst of the worst' scheme (see 'Appendix 1 – Cyber safety initiatives' for a summary of Telstra's current cyber safety initiatives).

[2] Australian Communications and Media Authority, 'Like, post, share—short report: Young Australians and online privacy', May 2013, p. 2
[3] Telstra survey, 'Australian Digital Natives 2014: Decoding attitudes and behaviours towards cyber safety', prepared by Pureprofile for Telstra, January 2014, p. 32
[4] Hinduja, S and Patchin, J.W. 'Bullying, Cyberbullying and Suicide', *Archives of Suicide Research*, volume 14, issue 3, 2010
[5] Dooley, J, Cross, D, Hearn, L and Treyvaud, R. *Review of Existing Australian and International Cyber-Safety Research*. Perth: Child Health Promotion Research Centre, Edith Cowan University, 2009

RESPONSE TO QUESTIONS IN THE SUBMISSION

Telstra has reviewed the Government's Enhancing Online Safety for Children discussion paper and is submitting responses to the questions based on both their potential bearing on Telstra as a business that supplies services to the community and where we feel we can add value to the discussion on important social policy issues.

Proposal 1: Establishing a Children's E-Safety Commissioner

Question 2

Considering the intended leadership role and functions of the Commissioner, which option would best serve to establish the Commissioner?

It is our view that if the Commissioner is to be created it should be an independent statutory office, receiving administrative support from an existing government agency with expertise in communications and digital technologies, such as the Department of Communications or the Australian Communications and Media Authority.

In determining the functional set up and scope of the Commissioner, we would hope that the spirit of the government's 'red tape reduction agenda' is considered. We advocate for the Commissioner to work within the existing compliance infrastructure to reduce any additional business and administrative impacts so that Telstra can continue to devote appropriate resources to supporting cyber safety education.

Proposal 2: Developing a complaints system, backed by legislation, to get harmful material down fast from large social media sites

Question 6

Is the coverage of social media sites proposed by the Government appropriate and workable?

We are not certain that the coverage of social media sites proposed by the Government is workable in its proposed form.

By regulating compliance by large social media sites only, whatever the final definition, those then defined as 'non-large social media sites' will not be captured if they do not volunteer to join the scheme. Confining the proposed scheme to only a few players who meet a size criterion means that the increasing number of smaller social networking sites will not be included. Therefore, the overall effectiveness of the complaints system would be questionable.

In recent years, we have begun to see displacement and fragmentation impact on the dominance of a few major social networking sites as users, particularly younger users, move to new sites, eg: Instagram and Tumblr; anonymous social networking sites, such as ask.fm and qooh.me; smartphone messenger apps, eg: KiK; and social apps, eg: Vine and Pheed. The social functionality of online games is also increasing.

Content can be copied and posted from one platform to another in an instant. So, too, can inappropriate content be posted to any social networking site no matter its size. Categorising sites by size and applying legislation to only a subset of sites means there is a risk of not capturing those users of smaller sites or users who have a variety of social networking accounts and move freely from large sites to small and back again.

The very intention of the scheme, to remove material targeted at or likely to cause harm to an Australian child, would be undermined if the government did not have the powers to have harmful material removed from smaller sites including those hosted offshore. The scheme needs to apply to all social networking sites, no matter their size, popularity or location (see our response to question 16 for suggestions on ways to encourage compliance by social media sites that lack an Australian presence).

Telstra also offers that whatever is decided, the scheme should apply to the social media provider rather than to the underlying carriage or internet service provider if they do not host the social media site.

Question 14

Is the test of 'material targeted at and likely to cause harm to an Australian child' appropriate?

The proposed statutory test would require that 'a reasonable person would consider that the material would be likely to cause harm or distress to the child.' Defining both 'harm' and 'distress' is challenging and the tolerance levels for both may vary as they are generic and relative terms that apply to that which is appropriate for a particular situation. Nonetheless, we prefer this descriptive as opposed to a prescriptive language approach, which presents challenges with events that are 'atypical' or 'outliers'. Prescriptive language is rarely 'one size fits all'. Hence the use of more descriptive, general language where each individual case is independently assessed and actioned, is the appropriate methodology for a framework intended to help manage human behaviour.

Question 16

What would be the best way of encouraging regulatory compliance by participating social media sites that lack an Australian presence?

The development of a standard industry approach, such as a registered code of conduct or a co-operative voluntary agreement, to address the process of complaints handling on social networking sites would be a good way to encourage industry participation and compliance as opposed to using a regulatory measure which may have no effect on an offshore provider. An example of a successful government/industry partnership is the European Union's Better Internet for Kids[6] that has the involvement of a coalition of CEOs from thirty-one technology, internet and telecommunications companies. In December 2011, in collaboration with the European Commission, they agreed to a Statement of Purpose with a 12 month plan of actions. The CEO Coalition was tasked to work on the following five areas:

- simple and robust reporting tools;
- age-appropriate privacy settings;
- wider use of content classification;
- wider availability and use of parental controls;
- effective takedown of child abuse material.

Subsequently, in 2013, the executives of the CEO Coalition agreed with the Commission to co-operate and not compete for a 'better Internet for kids' by, for example, looking for synergies in education and awareness programs.

Proposal 3: Examining whether there is a need for a new, simplified cyberbullying offence

The discussion paper references various options for enhancing protections against cyberbullying, including the creation of new criminal offences in this area. In Telstra's view, it will be important to ensure that any new offences are worded with clarity.

Internet service providers already operate under a host of legislative arrangements, including the Telecommunications Act, Privacy Act and the Telecommunications (Interception and Access) Act, that create obligations to protect customer information and provide reasonable assistance to government agencies. Any policy reform in the area of cyberbullying needs to be carefully designed not to replicate, conflict with or cause confusion around these existing obligations.

[6] https://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids

Further, any new legislative provisions should be carefully worded, both in terms of identifying what may constitute a cyberbullying offence and what powers an approved agency has to address such an offence. In particular, having reference to the wording of the New Zealand Bill mentioned in the discussion paper, it will be important that any concept of 'posting' relevant content (i.e. a digital communication that may constitute cyberbullying) is defined with sufficient precision so as to only pertain to the relevant actions of an individual that may be engaged in cyberbullying. This will ensure that websites to which relevant content is posted, and carriage service providers that transmit the content, cannot themselves be deemed to have 'posted' it.

It will also be appropriate to have regard to the position of website operators or service providers who, under the options raised in this section of the discussion paper, may be the subject of orders or notices to help remove relevant cyberbullying materials from the internet or other digital communications forums.

If an individual has posted relevant harmful comments to a website, or sent an SMS/email, and that individual 'poster' cannot be readily identified or tracked down, it is foreseeable that there may be attempts to bring a carriage service provider into the complaint because it is considered they will be more likely, or able, to take the steps considered necessary to end the cyberbullying. This might include organising for removal of a harmful communication from a public or closed forum.

A scenario may occur whereby a court or legislative body empowered to order the removal of non-consensual images or written content directs a carriage service provider to deny access to such internet sites posting harassing or defamatory type content. Likewise, where it is identified that a particular carriage service user is identified as transmitting or sending offensive or harassing material to a victimized party, the carriage service provider may be instructed to bar the service from use by a particular user.

This may result in significant cost and operational impost on the carriage service provider to either block sites and/or identify subscriber information associated with the posting of harassing or defamatory content. From a technical perspective, it is highly unlikely that a carriage service provider could identify an individual operating within a social media site. Telstra's systems are not configured to enable the 'routine' capture of forensic network traffic information or related communication such a level of scrutiny of our customers' online activities. Also, feedback from our customers suggests many would not welcome this degree of oversight by a service provider. As such,

service providers should not be placed in a position where they are required to, for example, request a social media site to takedown an account holder, posting or otherwise.

CONCLUSION

Enhancing users' media, digital and social literacy helps to mitigate online risks and foster effective and meaningful online participation. Nurturing the positive potential of technology use is dependent upon all members of the community being empowered to engage online in ways that are safe and supportive, enhance their wellbeing, and increase their opportunities. The challenge, therefore, is to support users to minimise the risks while promoting their digital participation and their capacity to derive the full benefits of connectivity.

It is Telstra's view that this can be best achieved through a combination of education, appropriate tools and industry codes or co-operative agreements. A continued focus on collaboration between key stakeholders and end users is likely to produce the most beneficial outcomes.

Telstra argues that any new regulation of social networking sites or changes to cyberbullying legislation should not impose any additional requirements on carriage or internet service providers to retain data, investigate users, block access to sites or request social network services to takedown an accountholder, posting or otherwise.

We look forward to further dialogue and collaboration with the Government on this important social policy area.

APPENDIX 1 – TELSTRA INITIATIVES

Education and partnerships

As an organisation that takes its corporate responsibilities seriously, Telstra supports and has developed a number of cyber safety initiatives for children, young people, parents and schools. These include:

- We have a range of consumer education material available for children, teenagers and parents that we distribute in hard copy format via school newsletters, libraries, schools and our workforce, and in digital format via our website. The topics cover cyberbullying, balancing screen time, protecting personal information, avoiding inappropriate content and digital footprints.
- We commission research on cyber safety issues, and develop pro-active education campaigns in response to the findings. An example of this is our recent research into the experience of young people growing up with an established media presence, and their expressed desire that their parents had engaged more fully with them regarding their online safety. In response to this, Telstra then ran a campaign encouraging parents to talk to their children about cyber safety.
- In 2012, the Telstra Foundation committed $8 million to a multi-year cyber safety partnership with the Alannah and Madeline Foundation to develop and deliver an eSmart Libraries framework to 1500 public libraries across Australia.
- We actively support a range of government and public awareness initiatives such as Safer Internet Day, National Day of Action Against Bullying and Violence, Stay Smart Online Awareness Week, and we run public cyber safety campaigns at Christmas and the commencement of the school year.
- In 2013, Telstra supported a Victorian Department of Education and Early Childhood Development program, 'Bully Stoppers', which aims to develop sustainable bullying prevention initiatives in schools.
- We are supporting the Geelong Football Club's 'Cyber Cats' program, empowering young people with knowledge to help counteract anti-social online behaviour.
- We co-chair the Technology and Wellbeing Roundtable with Reachout by Inspire Foundation and are a partner organisation of the Young and Well Co-operative Research Centre.
- In 2012/13, we trained 11,500 parents and high school students at our cyber safety seminars. We are now working with anti-bullying and youth leadership organisation, Project Rockit, to bring a range of digital citizenship workshops to schools and parents around the country.
- Telstra is the only Australasian member of the Family Online Safety Institute (FOSI), an international, non-profit organisation that convenes leaders in industry, government and the non-profit sectors to collaborate and innovate in order to develop new solutions and policies in the field of online safety.

Tools and network

In addition to our educational resources, Telstra offers parents and carers a suite of technical products designed to help make children and young people's online experience safer. Parental controls provide parents and carers with automated tools to help protect their children and set restrictions while using devices and services. Our products include:

- Smart Controls® – a consumer mobile phone safety product that allows parents to manage and apply restrictions to children's mobile services.
- BigPond® Parental Controls – a fixed and mobile broadband network product that helps protect users from websites and other internet activities that may not be suitable for their families. Parental controls include functions such as content filters and time-of-day restrictions.
- Telstra Safe Social™ – a social networking protection tool that allows parents to monitor their child's online activity no matter where, or how, a child uses their social network.

Telstra advocates that the use of parental controls needs to go hand-in-hand with a thoughtful decision by parents on their children's social, emotional and technical maturity, eg: whether their child is ready for a mobile phone, the teaching of basic mobile phone safety, the explanation of responsible mobile phone ownership and behaviour, and appropriate limits regarding use of such devices.

In terms of our network capabilities, Telstra is helping to combat child sexual exploitation by blocking the world's worst illegal child abuse and child exploitation websites. Telstra blocks a list of child abuse sites identified as being the 'worst of the worst' by international policing organisation Interpol. The blocking of illegal child abuse material applies to both Telstra's retail fixed and mobile internet services.

Telstra social media protocols

Telstra manages a range of social networking sites and we have an investment in social media use. Across all of our sites, we have clear community guidelines by which all community members must abide. Our moderator enforcement guidelines comprise a seven-stage process for moderators to be able to identify violations and to know and enact the escalation process as soon as violations occur. These guidelines ensure that all of our social networking sites are inclusive and inviting for everyone.

All staff must undertake a compulsory social media training course, the '3Rs of Social Media', to build awareness of the need to abide by company policy regarding social media use. Responsibilities

include: 'not post[ing] material that is obscene, defamatory, threatening, harassing, discriminatory or hateful to any person or entity.'[7]

[7] http://exchange.telstra.com.au/3rs/