



SUBMISSION OF THE FAMILY ONLINE SAFETY INSTITUTE¹

1. The Family Online Safety Institute is pleased to offer this submission to the Australian Government. It is our hope that these comments will provide the Department of Communications with relevant information to assist them in ensuring that Australian children are able to access the benefits of the online world safely. We appreciate the Government's interest and attention to these crucial issues and we look forward to the development of a comprehensive, successful online safety strategy.
2. The Family Online Safety Institute (FOSI) is an international, non-profit, membership organization² working to make the online world a safer place for children and their families. We achieve this by identifying and promoting the best practices, tools and methods in the field of online safety and privacy that also respect free speech. FOSI convenes leaders in industry, government and the non-profit sectors to collaborate and innovate new solutions and policies in the field of online safety. Through research, resources, events and special projects, FOSI promotes a culture of responsibility online and encourages a sense of digital citizenship for all. With roundtables, forums and conferences around the globe, FOSI plays an important role in driving the international debate.
3. Although FOSI currently only has offices in London and Washington, DC, a large number of the companies that we work with have a considerable presence in Australia, including Facebook, Google, Microsoft, Symantec, Twitter, Yahoo! and Telstra. As a result, we have increased our engagement in Australia over the past few years.
4. In 2010, FOSI contributed to the report of the Australian Parliament's Joint Select Committee on Cyber-Safety.³ In doing so, we stressed the importance of collaboration between all interested parties, believing that cooperation is the best way to ensure online safety for all. Additionally, FOSI has been consulted by delegations from Australian State governments,

¹ Stephen Balkam, CEO, Family Online Safety Institute. sbalkam@fosi.org
400 7th Street, NW, Suite 306, Washington, DC 20004 United States of America

² For more information see <http://www.fosi.org> FOSI members include: Amazon, AOL, AT&T, BAE Systems Detica, BT Retail, Comcast, Cyber Guardian, Disney, Eclipse, Entertainment Software Association, Facebook, France Telecom, Google, GSM Association, LinkedIn, Microsoft, Mind Candy, Motion Picture Association of America, NCTA, Nominum, Sprint, Symantec, Telecom Italia, Telstra, T-Mobile, The Wireless Foundation, Trend Micro, Twitter, Verizon, Vodafone and Yahoo!.

³ See http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=jcc/subs.htm at number 38

including that of the Law Reform Committee of the Parliament of Victoria, on issues such as sexting.⁴

5. More recently, in 2013, FOSI convened an event in Melbourne entitled ‘Global Digital Citizenship: Encouraging Safe and Responsible Use Online.’⁵ The conference was supported and hosted by Telstra, with additional support from Microsoft, Google, and the Australian Communications and Media Authority. It drew an audience of over 100 people and featured a day of panels and keynotes examining the key issues, challenges, and opportunities that the Internet provides children today.
6. The following day, representatives from relevant companies were brought together for a closed-door roundtable discussion focusing on areas of cooperation among industry to confront some of the issues that prevent children from fully embracing the online environment. Importantly, this also promoted a dialogue between those working in Australia and those who were visiting from the United States and Europe. The conclusion reached by participants of the roundtable was that a global approach, with attention to individual country sensitivities, would be the best way to confront many of the concerns that being online presents to families.
7. FOSI works to achieve its objectives by way of a multi-stakeholder approach to innovating best practices and sharing resources, and by actively engaging with policymakers around the world. In the United Kingdom, for example, FOSI has long been an active member of the UK Council on Child Internet Safety (UKCCIS)⁶ and now sits on the executive board. Since the inception of the European Commission’s CEO Coalition to Make the Internet a Better Place for Kids,⁷ FOSI has been a high-level participant and now works to promote the creation of new, innovative and educational content for children that focuses on the positive aspects of the Internet. In the United States, FOSI regularly engages at the federal and state level to provide resources and raise awareness about online safety efforts.
8. Additionally, FOSI has created comprehensive, user-friendly resources for professionals and consumers. For professionals and policymakers, we provide the Global Resource and Information Directory (GRID).⁸ GRID aggregates online safety laws, education initiatives, research and active organizations in over 190 countries, and is monitored by an editorial team to ensure accuracy after notable events or legislative shifts. As a resource, it is invaluable to allow for comparisons and learning opportunities on innovations from different countries, and we strongly encourage the Department of Communications to utilize this portal.
9. Furthermore, FOSI has developed a resource for parents, teachers and teenagers, called A Platform for Good,⁹ which is designed to allow users to ‘Connect, Share and Do Good’ online. It provides examples for teachers on how to incorporate technology into the classroom and gives children the opportunity to share stories on ways that they have used the Internet to

⁴ See

http://www.parliament.vic.gov.au/images/stories/committees/lawrefrom/isexting/LRC_Sexting_Final_Report.pdf

⁵ For more information see <http://www.fosi.org/fosi-events/melbourne-2013.html>

⁶ For more information see <https://www.gov.uk/government/policy-advisory-groups/uk-council-for-child-internet-safety-ukccis>

⁷ For more information see <http://ec.europa.eu/digital-agenda/en/creating-better-internet-kids>

⁸ For more information see <http://www.fosigrd.org>

⁹ For more information see <http://www.aplatformforgood.org>

help others or to enhance their own learning. Most importantly, A Platform for Good gives parents suggestions on how to talk to their children about staying safe online, including how to deal with cyberbullying, and provides interactive features and robust resources to help empower parents to become more engaged with the online lives of their children.

10. FOSI has conducted numerous research studies in the United States into the online behavior of teenagers and the concerns of parents, believing strongly that all policies from governments and industry, as well as initiatives, should have a solid foundation in fact. Our initial effort looked at the use of parental control tools,¹⁰ the second examined online behaviors and digital citizenship,¹¹ the third explored the varied attitudes towards online safety between the generations,¹² and in 2013 we looked at issues of identity theft as they applied to teenagers.¹³
11. In July 2011, FOSI and Hart Research Associates looked at the ways in which parents chose to monitor what their children were doing online and examined the awareness and use of technical parental control tools.¹⁴ Online safety remained an area where parents did not feel that their child was in danger, with 86% of parents reporting that they felt that their child was “very” or “somewhat” safe online. The proportion of parents who felt that their child is “very safe” decreased notably as the child grew older and spent more time online.
12. Findings showed that virtually all parents claimed to have talked to their children about their online behavior and the associated risks and benefits, but just over half of parents say they have used technological parental controls for Internet use. Among those parents who did not use parental controls, the most oft-cited reason was that they felt that they were unnecessary, owing to household rules or because they trusted their child to act safely and responsibly online. Nearly all (93%) parents said they had set rules or limits in one or more ways to safeguard their children online.
13. Notably, parents felt more knowledgeable about how to protect their children’s safety and privacy online when using a computer, as compared to smartphones or other handheld devices. Due to the constant increase in the use of mobile devices, this is an area in which more education and awareness raising should be encouraged. In response to these findings, FOSI created online safety contracts and other materials to help parents establish household rules and talk to their kids about setting limits for the sites they visit, amount of time they can spend online, and how they manage new devices.¹⁵
14. Also in 2011, FOSI and Pew Research Center examined online behavior and the notion of digital citizenship.¹⁶ The research showed, unsurprisingly, that social media had become

¹⁰ 2011, FOSI, Hart Research Associates. “Who Needs Parental Controls? A Survey Of Awareness, Attitudes, And Use Of Online Parental Controls.”

http://www.fosi.org/images/stories/research/fosi_hart_survey-report.pdf

¹¹ 2011, Pew Research Center, FOSI, Cable in the Classroom. “Teens, Kindness and Cruelty on Social Network Sites: How American teens navigate the new world of “digital citizenship””

<http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx>

¹² 2012, FOSI, Hart Research Associates. “The Online Generation Gap: Contrasting attitudes and behaviors of parents and teens.” <http://www.fosi.org/images/stories/research/hartreport-onlinegap-final.pdf>

¹³ 2013, FOSI, Hart Research Associates. “Teen Identity Theft: Fraud, Security and Steps Teens are Taking to Protect Themselves Online.” <http://www.fosi.org/files/Teen-Identity-Theft-online.pdf>

¹⁴ *Ibid.* 5

¹⁵ See <http://www.aplatformforgood.org>

¹⁶ *Ibid.* 6

pervasive in the lives of American teenagers. 95% of those surveyed were online, and of that 80% were social media users. The majority of teenagers using these services reported that their peers were largely kind to each other on these sites. However, 88% of users had witnessed other users being mean or cruel on social network sites, yet only 15% of teenage social media users had experienced such harassment themselves in the past 12 months.

15. Encouragingly, minors reported more positive personal outcomes than negative ones from interactions on social network sites: 78% report at least one good outcome, 65% had had an experience on a social network that made them feel good about themselves and 58% felt closer to another person because of an experience on a social networking site.
16. 95% of social media-using teenagers who had witnessed cruel behavior on the sites say they had seen others ignoring the mean actions, but 84% had seen people defend the person being bullied. Children continued to rely heavily on parents and peers for advice about online etiquette and coping with challenging experiences.
17. The Online Generation Gap study,¹⁷ undertaken in 2012, compared the attitudes of parents and children with respect to online safety. There was a stark difference between the amount of knowledge that parents had about their children's activities on the Internet, and the realities of what their children were actually doing. However, both teenagers and parents felt that they were generally safe online, and, importantly, minors exhibited an awareness of their digital reputation, with over 80% having actively adjusted their privacy settings. Of concern was the statistic that 43% of teenagers admitted to posting something online that they later came to regret, a fact that emphasises the importance of education around privacy and reputation management.
18. Following on from the Online Generation Gap study, FOSI and Hart Research conducted further investigation into a top concern listed by teens: identity theft. Over three quarters of teenagers are very or somewhat concerned about the privacy of their personal information being harmed by their online activity. The information that teens report as being most available online is their full name (75%), a photo (69%), their date of birth (54%), the name of their school (48%) and their e-mail address (47%). Furthermore, 34% of teens say they have shared one of their usernames and passwords with someone other than their parent or guardian.
19. However, teenagers are taking some steps to protect their information, 69% of teenagers report that they have set up one of their devices to auto-lock, which requires a password to be able to use it, and 56% of teens use a variety of passwords for their online accounts. They also expressed a willingness to consider further measures in safeguarding their information and devices.
20. It is essential to have an understanding of the environment in which children operate in order to create new initiatives and policies to enhance online safety and privacy. For now, it is hoped that the research findings will provide some constructive context to the Department in this consultation.
21. The Internet enhances the educational and social lives of children in Australia and around the world. Their use of media permits them to gain knowledge in a variety of new and engaging ways. Children are able to create and share their own content and express their ideas,

¹⁷ *Ibid.* 7

thoughts and experiences on a worldwide platform. The Internet allows for opportunities that take them far beyond their homes and communities; they are able to instantaneously explore the world, and immerse themselves in different cultures, geographies and periods in history. The skills children learn through their online exploration in early life prepare them for their future by providing knowledge as well as the digital abilities that are vital for functioning in a modern, technology-driven era.

22. The accompanying risks and challenges that go along with living in an online world cannot be discounted. Often, the skills and knowledge that children have about new media far exceeds that of their parents. There is illegal activity online, just as there is offline, and there is mean behavior and bullying. There is the possibility that children will be exposed to content and actions that are harmful to their development and well-being. At FOSI, we do not seek to diminish the existence of risks on the Internet, but rather to point out that they are no more prevalent online than offline, and do not necessarily require a completely different response. Just as talking to children and allowing them to have experiences is how they learn in the physical world, having an ongoing conversation with them as they engage in online exploration is the best way to protect them on the Internet.
23. Consequently, at FOSI, we believe the key to keeping children safe and ensuring that they have safe, productive and positive experiences on the Internet is to build a culture of responsibility online. This can only be accomplished if six separate entities work together to create a safer Internet. The key components are: 1) government; 2) industry; 3) parents; 4) law enforcement; 5) teachers; and 6) children.
24. Reasonable government support and oversight are essential components of this approach. An atmosphere of cooperation needs to be created amongst stakeholders. Cross-sector bodies, such as UKCCIS,¹⁸ bring together industry, non-profits, civil servants and ministers from government departments, educators, health professionals and researchers to develop strategies to counteract online challenges and emerging issues. Uniting relevant government departments also allows for consolidated governmental policies and approaches, rather than endowing just one person, or office, with total responsibility and power. Allowing detailed, considered input from a wide range of stakeholders with different areas of expertise permits and promotes the development of cohesive, constructive strategies that can be implemented across the ecosystem, thus better ensuring the safety of users. Increased funding for research into online behaviors and educational efforts that promote digital literacy and parental engagement are also essential.
25. Effective oversight of industry self-regulatory efforts allows for maximum innovation and development of creative solutions, while ensuring that industry continues to raise the bar in the field of online safety. As part of this, FOSI encourages robust and comprehensive industry self-regulation, discussing topics such as cyberbullying, the reporting of abuse, takedown requests and offensive material online. The roundtable that took place in Melbourne is a good example of this in action. As a membership organization, FOSI convenes leading technology companies, who often compete with one another on other issues or for market share, to discuss emerging issues, share approaches from around the world, and create best practices and new solutions to increase safety and privacy measures for children and adults alike.

¹⁸ *Ibid.* 6

26. There has never been a time when so many resources have been available for parents, grandparents, teachers, and caregivers to provide protection from online risks. All of the major operating systems and search engines provide family safety settings and mobile operators, social networks, and Internet Service Providers offer tools and options to help protect families. The popular social networks have tailored reporting structures that allow users to make complaints about content on their services. Company responses differ according to their systems and internal policies, but reports are assessed by experts and responded to appropriately. Imposing a further level of adjudication in addition to internal procedures, as the Department proposes, would result in a volume of complaints that would make the system unworkable and would devalue the initial reporting facilities provided by the social networks. Individual companies have nuanced responses that apply to the services they offer and they are often best placed to assess the grievances they receive.
27. Technological controls and processes cannot replace involved and empowered parents, but they do continue to be a part of the solution in keeping children as safe as possible online when used to the best of their potential. Technology develops at a rapid pace, and with each new development companies are working to stay current by creating new and innovative safety tools for parents and teachers.
28. Engaged and knowledgeable parents are vital to ensuring that children have a safe online experience. Providing and encouraging the use of online safety tools is a community-wide effort and each player in the online safety ecosystem can play a role in helping parents to learn about, and embrace, the tools available to them. Parents can be reached through educational campaigns provided by schools or the media, website safety blogs, school initiatives, and government outreach campaigns.
29. Law enforcement must be fully resourced and given the tools and training to combat the rise in cybercrime. Cross-border and cross-industry cooperation is vital to allow law enforcement officials to apprehend and prosecute those involved in illegal online activity. The ever-evolving nature of criminal activity via the Internet and the increase in the reporting of online criminal behavior, means that providing law enforcement with proper support is essential for the success of their efforts.
30. Superior technology training must be provided to all teachers. This will enable them to incorporate digital citizenship teaching across the curriculum, helping children navigate the online world safely and providing them with the skills to operate in an increasingly technical world.
31. Ideally, resilient children would make wise personal choices about the content they access and post online, the people they choose to engage with, and how they conduct themselves overall on the Internet. In order to achieve this culture of responsibility it is vital to teach children both media and digital literacy.
32. Children must be educated on how to operate as good digital citizens; to know about the rights and responsibilities that come with being online, to understand the consequences of sharing information on the Internet, and to empower them to make the right decisions when they see upsetting content or inappropriate behavior. Through teaching children to make good choices on the Internet, they can be better protected from the risks that exist online. The importance of avoiding a fear-based approach to education cannot be overemphasized. The skills that they learn through everyday experiences, with a foundation in proper education, will assist them throughout their digital lives, teaching them to be informed and resilient.

33. FOSI does not believe in, or endorse, new criminal legislation for cyberbullying. Regarding online harassment, existing statutes for offensive and inappropriate behavior are often adequate to deal with the very worst online actors, rather than legislating exclusively for norms that are constantly changing on the Internet. Criminalizing minors for youthful indiscretions that fail to reach the existing criminal standard is ill advised and unnecessary. Official responses to cyberbullying need to be moderated, nuanced, and appropriate to the circumstances.
34. It is important to note that research¹⁹ has shown that there is a broad spectrum of what has become known in the media as ‘cyberbullying.’ It ranges from friendly teasing to criminal harassment, with many degrees in between. Given this fact, and the often difficult and complicated lives of those involved, criminalization is not the appropriate response. Children should be taught not to engage in such misbehavior and to report it, through technical means or otherwise, when they see it. Concurrently, effective support and intervention networks must be created and maintained in order to assist those who perpetrate and those who are victims of bullying, both online and offline.
35. The government can best assist children through working as one part of the joined-up, engaged ecosystem. Their potential to raise awareness, direct funds to education and research, and to convene parties through multi-stakeholder bodies like UKCCIS, or the Consultative Working Group, is unrivalled. An open and productive dialogue between government and technology companies is often the best way to counteract many of the issues that arise online.
36. The responsibility of government to emphasize the positive aspects of the Internet and the opportunities that it provides must not be forgotten, nor diminished, in misguided attempts to pursue the impossible goal of keeping children completely safe online.
37. By ensuring the exemplary education of children, and informed and active parents, the Australian Government can begin to ensure the safety and privacy of all users, not just children. As a result of both formal education and informal experiences, Australian children will grow-up to take their place in the interconnected, global, digital world, and will do so safely.

¹⁹ 2011, Alice E. Marwick and danah boyd. “The Drama! Teen Conflict, Gossip, and Bullying in Networked Publics” http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926349