

PROTECTACHILD

RESPONSE TO DISCUSSION PAPER:

‘ENHANCING ONLINE SAFETY
FOR CHILDREN’

MARCH 2014

Contents

Introduction	3
Who we are and what we do.....	5
Media profile.....	6
What makes ProtectaChild different.....	7
Case studies	8
Case study one	8
Case study two	8
Context	9
Cyberbullying	10
Definition and characteristics	10
Incidence.....	11
Current approach by government.....	12
Our research	14
Methodology.....	14
Results	15
Children’s online activities	15
Where and how do kids get online, and what do they use?.....	15
Children’s online activity: program/websites/social media usage.....	16
Parents’ attitude towards and understanding of children’s online activity	16
Responses to specific issues in discussion paper	17
Improved coordination	17
Promoting more rapid removal of online content damaging to children	18
Support for parents and carers	18
Support for schools.....	19
Australian-based research on online safety and children	19

INTRODUCTION

In January 2014 the “Public consultation on Enhancing Online Safety for Children” was launched. This consultation was the logical consequence of the 16 November 2012 launch of an earlier discussion paper by the then Leader of the Opposition, Tony Abbott, on Online Safety for children. He invited comment from parents, schools, young people and industry about how children can safely participate online.

That call for input is a consequence of the work of the Coalition’s Online Safety Working Group, which found that parents and schools do not feel adequately equipped to protect children from online danger. The Coalition Government has also correctly identified that the previous Government’s ‘pre-occupation with its abandoned internet filter has meant that insufficient work has been undertaken to assist parents, carers and schools’.¹

ProtectaChild is pleased to have the opportunity to provide comment about this important issue. In this submission we have focussed on children’s use of social media and other online programs. We know that children and young people face many dangers and risks when they are online. We have developed an online tool that helps parents to protect their children against these dangers and risks, the details of which are outlined elsewhere in this submission. In doing so, we have examined many of the key issues at play in this complex policy challenge. We have consulted extensively with parents, teachers and others who confront this issue every day.

In 2011 we commissioned research about how children aged 10-16 use the internet; what parents know about potential dangers associated with this use; and strategies used by parents to monitor their children’s online activities. We have outlined the major findings from our own research in this submission and we are happy to share this knowledge with the Working Group. If the Working Group would like to use any part of our research, for example in a publication or some other output, please contact us first to seek permission. This is likely to be freely given but we do want to keep track of where and how this material is used.

In this document we describe what we believe is the largely haphazard approach by Australian governments to address children’s online safety. The last section of this submission responds to several of the specific ‘Matters for public discussion’ from the discussion paper, where they are relevant to our work, knowledge and experience.

We see the Opposition’s call for comment as a valuable opportunity to share the knowledge we have gained and hope that in this way we can contribute to a sensible policy outcome that protects children, and is practical and effective for schools and parents. In addition to this document, we would also be pleased to speak to the Committee or its members if further information is sought.

Today we have an impasse in relation to children’s online safety. Parents, teachers and government all have a role to play in ensuring that children are safe and should be working in close partnership. Instead there is little co-ordination. It’s our experience that parents, teachers and schools are doing their best to navigate child online

¹ Media Release, ‘Online Safety for Australian Children’, 16 November 2012.

safety, but there is a valid role for government to play in ensuring that all parties have the legal framework, knowledge and tools they need to play their own part.

We note that the discussion paper canvasses the ideal legal framework for child online safety, including penalties and consequences for breaches. Obviously this is important. Ideally however we would have a system where initial transgressions by children – or errors of judgement – are detected early. This should happen before reputations are irrevocably damaged or before a pattern of bullying is established – and well before a minor has to deal with the legal consequences of issues like slander or sexual harassment.

This brings us to one of the most important issues that we want to stress. We need a system where protecting children is not just about creating barriers to harmful influences or abuse. It should also be about parents being aware of their children's behaviour online, and having scope to quickly intervene if their children's actions towards others are undesirable or illegal.

WHO WE ARE AND WHAT WE DO

ProtectaChild was established in October 2011 by Jason Edwards, who is also the founder of marketing/media company cBox Pty Ltd.

ProtectaChild is a cloud-based monitoring application which provides an effective way to monitor children's social media online activity while still allowing them their privacy. ProtectaChild monitors; Facebook, YouTube, Twitter, MySpace, bebo, Instagram and Google+ by searching for keywords that can be associated with bullying, drugs, sexual content, depression etc. Parents have control and are empowered by being able to customise the keywords by submitting their own or omitting words that they do not deem to be of a dangerous nature.

As the ProtectaChild tool is cloud-based it simply links direct to the child's social networking page, meaning that there is no need to download any software; the parent / guardian simply signs up through the webpage (www.protectachild.com.au) and enters in the requested details. This also allows parents to monitor their child's online activity no matter which device the child is using (whether it be their own, a friends, or a public device) and parents are able to view alerts no matter where they are worldwide. Recently we identified a need by parents and users of the system for easier access to the feeds, and as a result, we have developed an App available for both iOS & Windows 8. Android will be coming shortly.

ProtectaChild also provides parents/guardians with 'profile validation' technology called Community Crowd Protection (CCP). This technology allows parents to "validate" their child's friend(s) which gives that friend a CCP rating; this is the cyber world's version of 'Neighbourhood Watch.'

ProtectaChild is designed to be an early warning system for parents that protects 10-16 year olds against potential online issues and threats including:

- Bullying
- Sexual predators
- Identity theft
- Reputation protection
- Unwanted exposure to adult themes such as drugs, alcohol or sexually explicit material

Importantly, it doesn't require parents to view all or almost all material that children are seeing or initiating. To do so is probably impossible for most parents. Not doing so also gives children a degree of privacy, albeit with important controls.

The starting point for ProtectaChild is the ProtectaPak, which helps parents set expectations and rules in relation to use of the internet and/or social media at home.

We are also beginning a trial involving 6-8000 users across a number of targeted schools in conjunction with the Computelec – a large national supplier to the educational market. They have arranged for a 6 month trial of the product to be available to a number of their schools. This trial will enable us to harvest considerable information in relation to the overall solution and implementation strategy and tweak any settings or measures where required.

MEDIA PROFILE

ProtectaChild has been approached by a number of media entities to discuss the product and its functionalities. Some recent examples of media coverage includes:

- NSW Station 2ST²
- Channel 7's Today Tonight³
- CIO magazine⁴

² <https://soundcloud.com/barrymac2st/jason-edwards-protectachild>

³ <http://au.news.yahoo.com/today-tonight/article/-/14776230/bully-program/>

⁴ http://www.cio.com.au/article/452270/anti-cyber-bullying_tool_creator_inks_deals_hardware_giants/

WHAT MAKES PROTECTACHILD DIFFERENT

Setup is simple and once access is authorised by the parent and child, ProtectaChild continuously scans for keywords that may be of concern and if suspicious or concerning content is detected then sends an email or if it is of a high concern, an SMS to the parent notifying them immediately of the issue. The parent can then view the context of the message or photo and decide if action is needed.

There is no need for the parent to know how to use Facebook or Twitter – or any of the other programs that are examined – or to have an account with, for example

ProtectaChild is markedly different to similar products on the market:

- It is Cloud based and so works on every internet accessible device: PC, Mac, iPad, iPhone, Android etc. It therefore may be used in any location, rather than being attached to one computer at home. (Many products require certain ports or firewall rules and/or admin rights to a machine to add any software, and this won't help monitoring by parents if for example a child accesses Facebook through a school supplied laptop. ProtectaChild installs its technology directly into Facebook etc, centrally overriding the device used to access the social media service and the location).
- It is designed to be adaptable to the ever changing landscape of social media trends and products – more social platforms are being added and coming online all the time.
- Monitoring occurs 24 hours a day.
- Parents have the ability to customise the keywords to accord with their own family values.
- It complements not replaces other school security systems currently being used, including home systems, corporate firewalls and/or agent based monitoring, and in particular schools who are working towards attaining e-Smart certification.
- It works extremely well within school settings where a community of people exist, by giving parents a remediation strategy and giving schools an insight via a dashboard as to the landscape of their environment.
- Combined with the ProtectaPak it works on the basis of open and transparent communication between child and parent/carer which is the core basis of best practice in this area.
- It is the only product on the market that has online grooming protection which is handled within the ProtectaChild ecosystem through the Community Crowd Protection – this module harvests the friends list, cross matches and asks parents for their input to ensure they are a part of the process.

CASE STUDIES

Case study one

Jamie, a 9 year-old boy, was constantly being bullied at school, including through social networking. He was too scared to tell his parents and teachers in fear that the bullying would increase and that his internet privileges would be taken away from him.

Jamie's parents purchased the ProtectaChild program and very quickly discovered the trouble that their son was having not only at school but also when he came home. They promptly arranged a meeting with the school and were dissatisfied with the response to their concern so chose to move schools. Unfortunately for Jamie the bullying continued, however, via the ProtectaChild tool, his parents were quickly made aware of the issue and could speak to the school early to rectify the situation.

Case study two

At the age of 13, Jack had difficulties in a relationship with a girl and was a great deal more upset than he had shown his family. Through ProtectaChild his parents discovered that his Facebook posts were not only of a depressive nature but also that they alluded to suicidal thoughts.

The alerts that the ProtectaChild program provided to the family enabled the parents to speak to their son and seek the help that he required at the time.

CONTEXT

Control or censorship of internet material has been a problematic policy issue for the current federal government which has simmered without resolution since the ALP took office in 2007. The central focus has been on preventing access to sites that have material that is considered inappropriate, and/or illegal, rather than on the behaviour of users of social media. With the site access issue still unresolved, there is growing concern about the effect of inappropriate behaviour by users of social media. In its extreme form it may become cyber stalking.

In December 2007 the Federal Government announced its intention to introduce an ASP-based filter to censor “inappropriate material” from the internet to protect children. Adults would be able to opt out of the filter. In May 2008 the government started an \$82 million “cyber safety plan” which included an additional mandatory filter with no opt-out provision

In October 2008 the Federal Government proposed extending internet censorship to a system of mandatory filtering of overseas websites which are or may be refused classification in Australia. The proposal attracted significant opposition and relatively few groups offered strong support.

The Opposition has attacked the filter proposal, claiming it is unworkable and that it is a slippery slope to more general censorship. It has also attracted vocal criticism from within the federal ALP, such as Senator Kate Lundy’s opposition to an opt-out clause. The Greens also oppose the approach and have argued that the filter as proposed is technologically unworkable.

In August 2010 the Coalition announced it would not vote for a filter, meaning it is unlikely it can happen. A November 2010 Department of Broadband Communications and the Digital Economy document indicated that the earliest date any new legislation could reach parliament was mid-2013.

Today this political background contributes to parents’ confusion about how to protect their children from online interaction that is inappropriate or illegal. Governments have made minimal efforts to address the growing issue of cyber stalking.

CYBERBULLYING

DEFINITION AND CHARACTERISTICS

There is a range of different definitions of cyberbullying in use, which has implications for research and policy. The Australian Parliament report of the Joint Select Committee on Cyber-Safety highlighted the importance of developing an appropriate definition for cyberbullying that is nationally consistent.

In the absence of this, the Australian Institute of Family Studies (AIFS) has used this definition which we believe is appropriate:

“... includes (but is not limited to): mean, nasty or threatening text messages/instant messages/pictures/video clips/emails that are sent directly to a person or others via a mobile phone or the Internet”.⁵

The AIFS notes that cyberbullying has a number of characteristics that are similar to offline or more ‘traditional forms of bullying, including:

- Power differential, repetition of behaviour and intent to harm
- Spreading rumours, making threats and derogatory comments

It notes that there are significant differences between cyber-bullying and other forms of bullying:

- Cyberbullying is more likely experienced outside of school, where offline bullying is more likely to be experienced in school
- Repetition of behaviour associated with bullying can be seen to have a different meaning in cyberbullying, as the sharing of materials can continue to occur long after the incident itself
- Younger students experience offline bullying more frequently than older students, but cyberbullying tends to be more common in the later years of high school (Cross, Shaw, Hearn, Epstein, Monks, Lester, & Thomas, 2009).
- Young people who experience cyberbullying may be less likely to tell someone than if they are bullied offline.
- Cyberbullying is perceived as anonymous, which may work to reduce the empathy felt by the young person who is engaging in bullying behaviour towards his/her targets. Young people are however most likely to be cyberbullied by people they already know.
- Young people who experience cyberbullying are less able to easily defend themselves or escape from cyberbullying, particularly as there is an infinite number of potential supporters of online bullying.

⁵ Definitions and characteristics of cyberbullying, Australian Institute of Family Studies, <http://www.aifs.gov.au/cfca/pubs/papers/a141868/03.html>, accessed 22 January 2013.

INCIDENCE

There are different statistics available regarding the incidence of cyberbullying. According to DoSomething.org, which claims to be Australia's largest nonprofit organisation for young people and social change:

- Nearly 43% of kids have been bullied online. 1 in 4 has had it happen more than once.
- 70% of students report seeing frequent bullying online.
- Over 80% of teens use a cell phone regularly, making it the most common medium for cyber bullying.
- 68% of teens agree that cyber bullying is a serious problem.
- 81% of young people think bullying online is easier to get away with than bullying in person.
- 90% of teens who have seen social-media bullying say they have ignored it. 84% have seen others tell cyber bullies to stop.
- Only 1 in 10 victims will inform a parent or trusted adult of their abuse.
- Girls are about twice as likely as boys to be victims and perpetrators of cyber bullying.
- About 58% of kids admit someone has said mean or hurtful things to them online. More than 4 out of 10 say it has happened more than once.
- About 75% have visited a website abusing another student.
- Bullying victims are 2 to 9 times more likely to consider committing suicide.⁶

⁶ <http://www.dosomething.org/tipsandtools/11-facts-about-cyber-bullying>, accessed 22 January 2013.

CURRENT APPROACH BY GOVERNMENT

Some legislation exists at a state level that is applicable to cyber stalking. This does not stop cyber stalking from happening but offers some legal redress in extreme cases. For most families, this would be an unlikely and last resort. Governments have initiated a more extensive range of policies and programs to tackle bullying, usually through some kind of online delivery, but these are generally aimed at bullying that occurs outside social media.

Two programs, recently announced by government, are of this kind. In March 2012 the state governments announced the Bullying No Way! Site as part of the National Day of Action Against Bullying and Violence. The site is intended to provide schools, children and teachers with skills to combat bullying.⁷

Similarly, on 31 July 2012 the federal Schools Minister, Peter Garrett, announced \$4 million in funding to help develop new online tools designed to tackle school bullying. It is intended that the tools will include an online information resource to help parents deal with bullying; a training module for parents and resources for student support staff.⁸

Governments have made minimal efforts to directly tackle cyber bullying.

In February 2013 the State Government of Victoria announced two new initiatives. On 4 February, it announced that thousands of Victorian school students would take part in an online conference 'dedicated to tackling cyber-bullying and promoting online safety'. It also announced that 1000 Victorian schools have signed up to the government's \$10.5 million eSmart initiative.⁹ eSmart was created by the Alannah and Madeline Foundation and is an educational program for schools to use with students to promote an understanding of online risks and encouraging appropriate behaviour.

Four weeks later the Government announced a social media online safety campaign called "It's There For Life!" The campaign involved schools and youth organisations such as Scouts and Guides to warn of the dangers of posting personal information online or sending it to others. The campaign will involve a competition, information sheets and targeted messages.¹⁰

More generally the approach in Australia and overseas is to urge parents to be vigilant and to monitor their children's use of social media, for example by friending their children through Facebook. A similar approach is used by some schools. For example:

⁷ 'Website tackles bullying among children', AAP, 16 March 2012.

⁸ Lanai Vasek, 'Funds for online anti-bullying tools', *The Australian*, 31 July 2012.

⁹ Tackling the scourge of online cyber-bullies, The Hon Martin Dixon MP, media release, 4 February 2013.

¹⁰ When you post or share, It's There For Life!, The Hon Ryan Smith MP, media release, 28 February 2013.

- President Barack Obama and Michelle Obama urged parents and students to work together to stamp out cyber bullying, telling kids to block cyberbullies, not retaliate and to keep the evidence. They cited an American study of 2,000 teenagers that suggested that 20% had considered suicide as a result of cyber bullying.¹¹
- The Australian Institute of Family Studies, in an Australian Government media release in June 2012, urged parents to ensure their children did not have social networking accounts when aged less than 13, and to monitor their usage and discuss it with them. The release included the claim that 7-20% of school-aged children and young people in Australia have experienced cyber bullying.¹²

These approaches are well meaning but probably ineffectual.

They don't appear to take into account the sheer amount of time involved in monitoring a teenager's various social networking accounts, and they generally assume that the behavior parents will be looking for is bullying of their children by others, rather than their own children inappropriately using social media.

Nor do they allow for the unfortunately common practice of children setting up more than one profile; one is considered by the children to be suitable for parental viewing, and an additional profile or profiles are maintained without parents' knowledge. (ProtectaChild uses a combination of technology and mobilising the online community to locate duplicate profiles and alert parents to this fact. This happens in two ways. First, activity will usually drop on the duplicate, meaning the parent will get no or few alerts. In addition, the duplicate profile will usually be linked to other students already on the system, which means it will be questioned and escalated by the system as being a duplicate. It is then the role of parents to respond to this behaviour.

A key issue identified by ProtectaChild is the sheer lack of technical knowledge to perform simple monitoring measures by the vast majority of parents. Due to the rapidly changing landscape, parents are often bewildered by the technology and don't have a starting point. By combining a simple and effective interface with the proliferation of 'App' technology through the ProtectaChild app, this brings down the level of expertise required to a minimal requirement to empower parents to take back some control in this area.

What is also missing from this discussion is online tools that detect behaviors before they become a habit or a trend. There is an opportunity to start the conversation about the need for these tools, and for government assistance to provide them, as part of the more general bullying debate.

¹¹ *The Obamas Tackle Cyberbullying and Urge Parents To Take Responsibility*, 9 March 2011, <http://www.parenting.com/blogs/screen-play/jeana-lee-tahnk/obamas-tackle-cyberbullying-and-urge-parents-take-responsibility>, viewed 1 August 2012.

¹² Schools and families critical to tackling cyberbullying, Australian Institute of Family Studies, media release, 1 June 2012.

OUR RESEARCH

In December 2011 we commissioned the Mobium Group to conduct research to examine the following:

- Parents' awareness of the potential danger of children's online activities
- Parents' knowledge and concern about their children's online activities
- Strategies used by parents to monitor children's online activities
- Children's online activity: which sites are visited; how often; total time spent online

METHODOLOGY

The total sample size was 520. The primary audience was parents of children aged 10 – 16 and the sample was split with a weighting of 50% for public schools and 50% for private schools. 53% of respondents were female and the remainder were male.

The survey was online and based on random selection and included respondents from around Australia. The data was collated over six days in December 2011.

Based on responses about the number of children living within the household of each respondent, the sample encompassed 706 children aged 10 – 16 with 52% female and the remainder male.

Responses indicated that 70% of schools had a compulsory computer program for students, with 21% indicated there was no such program and 9% not knowing. Of the schools with a program, 94% of private schools had a compulsory computer program compared with 47% of public schools.

Please contact us if you are interested in more detail on the respondents' or children's profiles.

RESULTS

Children's online activities

Predictably, children use the internet frequently and with enthusiasm. 66% used it every day, 27% used it most days, 6% used it a few days a week and 1% used it once a week. There was a strong correlation between age and usage; as age increases, the usage frequently grows to peak around 80% daily use from 16-18 years.

Usage Frequency - Age							
N = 706	10	11	12	13	14	15	16
Every day	42%	54%	63%	70%	80%	78%	82%
Most days	35%	40%	30%	25%	17%	21%	16%
A few days	19%	8%	4%	5%	3%	1%	2%
Once a week	4%	0%	1%	0%	0%	0%	0%

Where and how do kids get online, and what do they use?

Across all age groups, home and school are the usual locations for internet connection. 98% of online users do so from home, 86% at school, 25% at a friend's home, 16% at the library and 7% indicated other.

As age increases into the teenage years, access from other channels increases with more than a quarter of 14-16 year olds accessing the internet at friends' homes and similar numbers at a library.

Mobile phones are also prominent among older teenagers.

Location - Age							
N = 706	10	11	12	13	14	15	16
At school	96%	100%	99%	100%	98%	98%	100%
At home	77%	82%	84%	80%	78%	86%	88%
At friends	14%	20%	18%	20%	24%	26%	34%
At Library	7%	8%	9%	18%	17%	26%	28%
Other	2%	0%	2%	2%	9%	19%	26%

Our research also showed that computers are by far the most prevalent device for internet connection but there is a range of alternate modes including mobile phones (41%), music players (29%) and game consoles (26%) as the next most common. Nearly 70% of children have one device besides a computer that can access the internet and more than one in five has three or more alternatives.

Children's online activity: program/websites/social media usage

Parents were asked to estimate how frequently their children use a range of programs, websites and social media. According to parents, 86% of children aged 10-16 use YouTube and seven in ten use Facebook. 81% use online games and 80% use email.

Messaging programs such as Skype (41%) and msn (39%) had moderate levels of interaction. Myspace (16%) and Twitter (15%) had comparatively much lower levels of interaction.

We also examined in detail how often children use each form of program, websites etc. In the interests of brevity we have not including this data in this submission but we are happy to provide it if requested.

Parents' attitude towards and understanding of children's online activity

In this section of the survey, parents were asked to review statements and indicate how strongly they agreed or disagreed. Again, in the interests of brevity we have not included all the response material we have but if the Committee is interested in seeing this we would be pleased to provide it.

In summary:

- Most parents say they are highly comfortable with the levels of communication, scrutiny and monitoring of their child's online activity. There is an optimistic view that they are in control of their children's online activity.
- Overall 94% of parents say they have 'a good understanding about prevalent online issues for children', 90% know 'safeguards' and 79% say they 'currently use safeguards to make their children safe online'.
- 85% say they are 'confident' they know all the online accounts and social media used by their children and 90% state that their children's online friends are legitimate.
- 82% say they regularly monitor their children's online activity.
- There is a higher level of concern about children posting 'something online that makes them vulnerable without knowing it', with 38% indicating it is a potential issue.

RESPONSES TO SPECIFIC ISSUES IN DISCUSSION PAPER

Improved coordination

The Coalition has floated the idea of an independent agency or Commissioner-led body, such as a 'Children's e-Safety Commissioner', charged with the role of co-ordinating a national response to online safety. Comment is invited on this and other details such as the role, nature and operation of this kind of agency or Commissioner; and whether any existing agency has capacity to take on this role.

We understand the attraction of this idea but are concerned that it is taking responsibility away from parents. Paradoxically it would also mean further delay in dealing with the problem of online safety. It would take time to set up new infrastructure and to determine responsibilities. We note also that there are existing bodies/commissioners who could probably take on such a role if it were necessary. Child safety commissioners are already appointed in various states. In Victoria, the role of Child Safety Commissioner was created in late 2012 and Bernie Geary was appointed to the role in February 2013. In April 2012 the Gillard Government announced that a National Children's Commissioner would be established within the Australian Human Rights Commission. This was a key action from the Government's National Framework for Protecting Australia's Children 2009-2020.

To date, much of the 'co-ordinating' role played by government could be described as broadly educational. Generally this has boiled down to setting up websites as a way of delivering reminders and tips to parents - that they should monitor their children's online use and discuss appropriate use with their children. Educational programs within schools are the other 'co-ordinating' role played by government. This has more value, in that it is teaching children awareness of the dangers and appropriate online behaviour and etiquette.

We believe that there is already a sufficient framework for oversighting online safety. What is needed is action to ensure parents and schools have the practical support to monitor and intervene when needed. Parents need a realistic way to know what their kids are doing online, which doesn't involve examining every email, tweet or Facebook update. Ideally this would be co-ordinated with or through schools. There is a role for government to play in identifying products and using their buying power that equips parents, and to a lesser extent teachers, to play their part.

Promoting more rapid removal of online content damaging to children

We understand that this section concerns material that goes well beyond that generated by children for other children to see. We also acknowledge the point made on page 6 of the Discussion Paper that the problem ‘is that some internet activities and content are not illegal per se, but can be nevertheless detrimental to children if used in a deliberately malevolent way’. Online comments and Facebook posts are given as very good examples of this.

Again, this is an area where we believe parents (and to a lesser extent, schools) should be given the tools to identify this kind of material so that they can intervene early, and in an appropriate way. Generally this will mean explaining why the material is inappropriate, what its likely impact would be, and ensuring it is removed.

Our observation is that very often online abuse starts very subtly through teasing, some of which is quite innocent in nature and which occurs between online friends who know each other offline. If left unchecked it can quickly get out of hand. Due to the very public nature of many forms of social media, teasing or a silly or hurtful comment can quickly turn into serious bullying, especially when the mob mentality of the internet becomes involved. An initial exchange between two people who know each other - that is possibly innocent or at worst, careless – can easily become an ugly crowd event that draws in potentially thousand of people who don’t know the original protagonists or the real meaning of the initial exchange. Material that is objectionable, offense or defamatory is not sufficient to trigger a take-down notice.

We need a better way for parents and where appropriate teachers to intervene well before anyone is contemplating a take-down notice. By then, the damage has often been done even if the offending material is made to disappear. We need a way to head off these situations early.

One approach is to ensure that companies like ProtectaChild have continued access to the backend systems of social media programs through APIs, in the same way that we do with Facebook and other programs. This would mean that when another online program emerges and is popular with children – and especially if it is directly marketed to children – then parents could be assured of a plug-in that gives them oversight, without having to literally look at every word. In other words, the safety feature would become part of the new social media product’s license to operate in Australia.

Support for parents and carers

We support the principal behind Coalition’s proposal to enable parents and schools to purchase products from a range of vendors and operators that meet national standards for online safety for children. Parents and schools have many products from which to choose and for many this is a confusing marketplace. We also believe it makes sense for government to use the benefits of large scale procurement to help give greater value to parents and schools.

We note that ‘a key element of the standards would be to require that a product be sold with appropriate parental control tools enabled as the default setting’. This approach seems to anticipate a situation where every device has some kind of parental control device. Our research shows that children use devices in a range of settings, therefore it may not be possible to ensure that the device is on every product a child uses. We also question whether the kind of devices that the Coalition has in mind have the subtlety to detect some words.

This could be relatively easily achieved via the mandatory inclusion of an API that is made accessible to organisations such as ProtectaChild that (via an approval process) automatically registers children's accounts and includes them for alert based monitoring.

We submit that it makes sense for any incoming Coalition government to do what other governments have done in similar situations: conduct a series of trials with schools and parents to test products that are available today, and then compare the results and feedback.

Support for schools

We agree with the comments made on page 10 of the Discussion Paper about a range of different programs and tools being used by schools, with a great deal of diversity in terms of what the programs deliver and to whom. We too are conscious that for some schools there is a 'tick the box' approach that is more focussed on being seen to do something than delivering a response that really works. For many schools, this is a very new area and one that is fraught with danger, risk and expense.

As we have indicated earlier, ideally we would have a strong working relationship between homes and schools in relation to online safety. This would be an extension of the more general approach to educating children, and it would also be a practical acknowledgement that online devices are portable, and that online technology is an increasingly common educational tool.

Creating a community based culture within a school allows for rapid addressing and escalation of issues if & when they arise. ProtectaChild can easily integrate with these entities and currently provides a dashboard which anonymises and aggregates collective data together of the schools current state of play in terms of alerts, community crowd protection (groomer detection), and activity.

If so desired, ProtectaChild is also capable of providing a linked connection to the school that a child attends for the purposes of parental escalation in the case of a cyber bullying instance. Anecdotally, this is by far the quickest and most efficient method (and frequently the only method) of addressing cyber bullying effectively.

We support the inclusion of a stronger online safety component in the National Safe Schools Framework. We argue that without providing schools with the tools to deliver this, this will be of minimal real value.

Australian-based research on online safety and children

We agree that there is a surprisingly large amount that is unknown about the impact of 'internet immersion' on the health and wellbeing of young children. We would add that there are other gaps in knowledge about children's internet use and the role and perceptions of their parents. This is one reason why we commissioned our own research. We support additional and ongoing research in this area and would happily collaborate in exploring new areas of research.