SUBMISSION No. 88

CONTENTS

Internet Industry Association

To: The Secretary of the Joint Select Committee on Cyber-Safety

via jscc@aph.gov.au

9 July 2010

SUBMISSION BY THE INTERNET INDUSTRY ASSOCIATION (IIA)

We thank the Committee for the opportunity to provide this submission which:

- outlines the IIA's views on relevant aspects of cybersafety,
- highlights relevant research findings
- argues for funding of more Australian research, and
- presents examples of IIA's work in this area over the past decade or so.

ABOUT THE IIA

The Internet Industry Association is Australia's national representative Internet industry organisation.

Established in 1995, we represent over 150[1] multinational, national and small businesses including telecommunications carriers, search engines, content creators and publishers, social networking sites, web developers, e-commerce traders and solutions providers, hardware vendors, systems integrators, technology law firms, ISPs, educational and training institutions, Internet research analysts and a range of other businesses providing professional and technical support services.

Our vision is to promote a faster, safer, fairer and more trusted internet for Australia. Consistent with our charter, the IIA provides policy input to government and advocacy on a range of business and regulatory issues, to promote laws and initiatives enhancing access, equity, reliability and growth of the internet within Australia.

In the 15 years since our formation we have provided leadership in:

- formulating internet policy for industry
- setting industry standards and codes of practice
- advising on legislation

[1] See Appendix 3 for full list of members.

- assisting parliamentary inquiries
- instigating public empowerment initiatives
- participating in key committee roles; and
- promoting joint industry/government cooperation.

THE NATURE, PREVALENCE, IMPLICATIONS OF AND LEVEL OF RISK ASSOCIATED WITH CYBERSAFETY

In considering the risks of online activity particularly in relation to children, the IIA urges the Committee to review the available research evidence before drawing firm conclusions as to the need for further policy reform, particularly of a legislative nature.

The most prominent of these studies internationally is the *EU Kids Online Project* which examined cultural, contextual and risk issues in children's safe use of the internet and new media across 21 countries.[2]

The IIA encourages the Committee to also consider the *Review of Existing Australian and International Cyber-Safety Research* [3] by the Child Health Promotion Research Centre at Edith Cowan University published in May 2009.

In addition, we commend the US Internet Safety Technical Task Force, *Enhancing Child Safety and Online Technologies - Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States (December 2008*).[4]

The US Internet Safety Technical Task Force (ISTTF) concluded "…Minors are not equally at risk online. Those who are most at risk often engage in risky behaviours and have difficulties in other parts of their lives. The psychosocial makeup of and family dynamics surrounding particular minors are better predictors of risk than the use of specific media or technologies."[5]

The literature review[6] from the IITF's research advisory board, for example, question the pervasive view in the media that sex crimes on the internet are on the increase. In fact it found that internet sex crimes against minors have *not* overtaken the number of unmediated sex crimes against minors *nor* have they contributed to a rise in such crimes.

> "Yet the increased popularity of the Internet in the United States has not been correlated with an overall increase in reported sexual offenses; overall sexual offenses against children have gone steadily down in the last 18 years (National Center for Missing and Exploited Children 2006).

[2] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

[3] http://www.dbcde.gov.au/__data/assets/pdf_file/0004/119416/ECU_Review_of_existing_Australian_and_international_cyber-safety_research.pdf

[4] http://cyber.law.harvard.edu/pubrelease/isttf/

[5] ibid p.4

[6] ibid Appendix C of *report*

> "State reported statistics show a –53% change in reports of sexual offenses against children from 1992 to 2006 (Calpin 2006; Finkelhor and Jones 2008), which Finkelhor (2008) argues is both significant and real. Furthermore, sex crimes against youth not involving the Internet outweigh those that do; Internet-initiated statutory relationships are greatly outnumbered by ones initiated offline (Snyder and Sickmund 2006; Wolak et al. 2003b) and the majority of sexual molestations are perpetrated primarily by those the victim knows offline, mainly by family members or acquaintances (Snyder and Sickmund 2006)."

In June this year, the US Government's National Telecommunications and Information Administration released its Online Safety and Technology Working Group (OSTWG) final report to Congress entitled, "*Youth Safety on a Living Internet.*"[7]

This US government taskforce comprised over 30 experts from academia, industry, advocacy groups and think tanks. It was established pursuant to "Protecting Children in the 21st Century Act," (part of the ''Broadband Data Improvement Act',' Pub. L. No. 110-385) and its mission was to review and evaluate:

- The status of industry efforts to promote online safety through educational efforts, parental control technology, blocking and filtering software, age-appropriate labels for content or other technologies or initiatives designed to promote a safe online environment for children;

- The status of industry efforts to promote online safety among providers of electronic communications services and remote computing services by reporting apparent child pornography, including any obstacles to such reporting;

- The practices of electronic communications service providers and remote computing service providers related to record retention in connection with crimes against children; and,

- The development of technologies to help parents shield their children from inappropriate material on the Internet.

The taskforce concluded there were no easy technical solutions to manage online child safety concerns. Instead it opted for a diverse toolbox - a "layered approach". In particular, it found:-

- There is no one-size-fits-all, once-and-for-all solution to providing children with every aspect of online child safety. Rather, it takes a comprehensive "toolbox" from which parents, educators, and other safety providers can choose tools appropriate to children's developmental stages and life circumstances, as they grow. That toolbox needs to include safety education, "parental control" technologies such as filtering and monitoring, safety features on connected devices and in online services, media ratings, family and school policy, and government policy. In essence, any solution to online safety must be holistic in nature and multi-dimensional in breadth.

- To youth, social media and technologies are not something extra added on to their lives; they're embedded in their lives. Their offline and online lives have

[7] http://www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf

converged into one life. They are socialising in various environments, using various digital and real-life "tools," from face-to-face gatherings to cell phones to social network sites, to name just a few.

- Because the Internet is increasingly user-driven, with its "content" changing real-time, users become stakeholders in their own well-being online. Their own behaviour online can lead to a full range of experiences, from positive to victimisation, pointing to the increasingly important role of safety education for children as well as their caregivers. Future task forces need to consider protective *education* as well as protective technology.

- The Internet is, in effect, a "living thing," its content a constantly changing reflection not only of a constantly changing humanity but also its individual and collective publications, productions, thoughts, behaviours, and sociality.

The IIA regards the findings of this report as a reliable starting point for tackling the challenges of cybersafety in the 21st century.

The OSTWG's subcommittee on Internet Safety Education concluded that the traditional issues which parents were concerned with such as child predators have been overtaken by the newer issues from the massive adoption of social networking sites.

These new issues include cyberbullying or 'sexting'. Rather than a single solution to combat these issues, they argued the government needs to look at various methods.

The "levels of prevention" method promises a tailored and scalable approach that would also work with non-fear-based, social-norms education, and promotes and establish a baseline norm of good behaviour online.

OSTWG's proposed creation of a "Digital Literacy Corps" which would help educate children from K-12 is worth also considering and resourcing in Australia. Our Safer Internet Group is exploring options to fund pilot trials in this regard.

Additionally digital literacy should become an integral part of K-12 education.

The IIA cannot over-emphasise the need to support education that has been shown to work with clear and positive outcomes. It is too easy to fund a package of conventional lecture-style programs that miss their mark with their target groups or fail to achieve real changes in terms of cultivating our children's ability to gain from the richness of the internet while avoiding many of its pitfalls. Instead, programs must be predicated on achieving appropriate behavioural change among susceptible individuals.

This issue was well documented in Lisa M. Jones's recent essay, *The Future of Internet Safety Education: Critical Lessons from Four Decades of Youth Drug Abuse Prevention.*[8]

Jones urges internet safety education proponents to study the history of youth drug and alcohol abuse prevention, in particular. She notes the striking similarities in the political contexts of the two initiatives and the intensity of public concern. She identifies parallels in our eagerness to prevent Internet victimization and early rushed efforts to prevent youth drug abuse in the 1970s and 80s. Internet safety proponents have a real opportunity to avoid reinventing the wheel.

[8] http://publius.cc/future_internet_safety_education_critical_lessons_four_decades_youth_drug_abuse_prevention

She finds that lecture formats are common as are frightening stories of Internet victimisation used to try and compel youth into changing the ways they interact on the Internet. While entertaining and attention-grabbing, she argues that research suggests that such messages do little to get youth to change how they are behaving.

She concludes that internet safety programs that contribute to good outcomes support:

1) explicit theoretical design;
2) defined purposes and goals;
3) interactive learning; or
4) multiple exposures to educational messages.

On the other hand, less effective programs tend to:

1) rely on lectures and presentation formats;
2) focus only on knowledge building and changing attitudes; or
3) use fear tactics.

While the online environment experienced by Australian children is not dissimilar to those of other modern Western economies, it is imperative that more local research is undertaken to provide a credible evidence base for future policy. There is a central role for Government in supporting such research so that the goal of evidenced based policy is realisable.

THE NEED FOR FURTHER DOMESTIC RESEARCH

The IIA is currently liaising with three eminent researchers in the area of children's experiences with the new media.

Professor Lelia Green from Edith Cowan University and one of the researchers seeking to undertake the study explains the background:

> *The proposed project which requires significant funding if it is to proceed, is not just research into what children do, and what children have seen, but also whether and to what extent any of the actions or experiences are distressing or troublesome. This is a study of resilience as well as of behaviour. The materials have been extensively validated by the EU Kids Online team and the interviews with the 25,000 children in Europe are nearing completion.*
>
> *Ipsos […] or their affiliates, have run the project in each of the other 25 countries and have checked capacity and availability to carry out an absolutely consistent equivalent project in Australia. Sonia Livingstone describes the importance of this research in the following terms: Funded by the EC's Safer Internet Programme, EU Kids Online II (2009-11) is a collaborative knowledge enhancement project involving some 70 researchers in 25 countries across Europe and spanning diverse disciplines, methodological expertise and research specialisms.*
>
> *Distinctively, this new project is based on a strong multidisciplinary theoretical framework developed to guide the construction of a unique and substantial dataset. Key features of the study design include: survey administration in homes, face to face with children, and a self-completion section for sensitive questions; random stratified survey sampling of 1000 children (9-16 years old) per country who use the internet; direct comparison questions to the parent most involved in their internet use; detailed*

questions on psychological vulnerability, social support and forms of safety mediation; equivalent questions to compare varieties of online risk, including comparisons with offline risk; and follow up questions pursue how children respond to or cope with online risk.

This design will add to the evidence base by providing, during 2010-11:

- *an account of children's experiences, including findings for new media use across locations and platforms;*
- *comparison across different online risks and strategies of safety mediation, as reported by children and by their parents, contexualised in relation to offline risks;*
- *new findings comparing child as victim and perpetrator, on risk-taking and coping (building resilience);*
- *directly comparable data across countries to permit analysis of national and regional differences.*

In sum, these EU Kids Online II findings are likely to show that online technologies afford children significant and diverse risk experiences, and that these may cause harm under certain circumstances and to certain children unless effective mechanisms of mediation (parental, school, peer, other) are available to prevent such encounters or mitigate against negative consequences.

The Department of Broadband Communications and the Digital Economy (DBCDE) declined the opportunity to be involved in this research on 19/05 with the relevant First Assistant Secretary arguing that the DBCDE had commissioned "an extensive survey of teachers and parents. This research has been designed specifically to inform policy development in Australia. While not exactly the same, there is considerable overlap between the research we have already commissioned and your proposal"; even though DBCDE have no plans to interview a single child or young person.

The EC Safer Internet Program has funded EU Kids Online II to the tune of €2.5M. In most countries it is the government and regulators that are most keen to discover just how vulnerable or resilient the children in their nation are, in comparison with the 24 other nations involved in the study.

The fact that the Australian government has committed $125.8M over four years (2008-11) to 'protect children', but walked away from the opportunity to research comparative risks for Australian kids in a way that benchmarks them against 25 other nations, creates a vacuum in evidence-based policy discussion that the internet industry in Australia could immediately address and reap value from for the next two years as the comparative research is released.

We may well have very resilient children in Australia: we may be operating in an exemplary and empowering environment for kids online. But at the moment we would have no robust evidence of this.

INDUSTRY EFFORTS TO PROMOTE CHILD SAFETY ONLINE

In addition to the measures implemented by our individual members, the IIA has responded to emerging issues with the development of best practice standards. We believe these moves to be among the most advanced in the world, particularly in relation to their comprehensiveness and co-regulatory nature.

Co-regulation allows for flexible code based responses to be developed and applied, while relying on underpinning legislation to assist in their application across entire industry sectors. They thus overcome the static effects of pure legislative 'solutions' which cannot adapt quickly enough to meet the challenges presented by rapidly changing technologies.

Under the *Broadcasting Services Act 1992* which provides the legislative framework for co-regulation in matters of online content, the Australian Communications and Media Authority (ACMA) has the power to investigate complaints relating to Prohibited Content or Potential Prohibited Content and to monitor compliance with Codes. Contravention of a requirement of a Code by a person covered by the Code may be the subject of a warning by ACMA or a direction by ACMA to that person to comply with the Code and, if a direction by ACMA is not complied with, enforcement action by ACMA and imposition of penalties pursuant to Schedule 5 and (since 2006) Schedule 7 of the Act.

IIA's code making activities (beyond our initial self regulatory codes) first started in 1999, when we developed and registered three ISP Codes of Practice. The 2005 revisions to the Codes rationalised their number and incorporated new provisions relating to mobile services is current and remains in force.[9]

In 2001, the IIA developed and registered the Interactive Gambling Code of Practice in response to the Interactive Gambling Act 2001. This Code also applies to ISPs in Australia and is also an enforceable co-regulatory instrument.

In 2002, the IIA introduced the **Family Friendly ISP** scheme. This scheme accredits ISPs complying with best practice standards providing branding rights in return for adherence to best practices. Related to this is our accredited filter scheme where ISPs make available filters that are tested in accordance with criteria that we have developed jointly with the regulator, ACMA. Under the present industry codes of practice, ISPs are required to make those filters available to their users. **Appendix 1** outlines this scheme.

The Family Friendly ISP Scheme was bolstered in 2004 with the commencement of the **IIA Family Friendly Filter** scheme. This Scheme provides an objective basis for the assessment and recommendation of filters to end users. Accredited filters must pass independent testing according to criteria jointly agreed by the IIA and ACMA. ISPs that wish to comply with the IIA's registered codes of practice must make an accredited (IIA Family Friendly) filter or filtered service available to users on an opt-in basis.[10]

Amendments to the *Broadcasting Services Act* in 2006 saw a separation of the responsibilities of ISPs and Content Hosts necessitating the formulation and registration of a further industry Code, registered by ACMA in 2008. The Content Services Code of Practice with ACMA is also an enforceable industry wide code underpinned by legislation.

[9] The full Code can be viewed at http://www.iia.net.au/images/resources/pdf/iia_code_2005.pdf

[10] A list of currently approved Family Friendly Filters is available on IIA's site at www.iia.net.au

The Code provides the means for locally-based commercial content service providers and live content service providers to ensure that potentially restricted commercial stored content services or live content provided by commercial content services now comply with Australian classification schemes. The Code promotes safer online experiences for the community (particularly children) through workable industry regulation. It supports the local content provider industry with clear guidelines in line with internationally accepted practices.

In particular, the Code provides industry with guidance on:

- handling complaints (Part C),
- taking-down notified content or content services (Part D)
- promoting online safety for Australian families (Part E)
- implementing restricted access systems for some content services (Part F); and
- regulating certain chat services (Part G).[11]

In addition to these efforts, the IIA recently provided to the Consultative Working Group on Cybersafety (on which we are represented) a concise list of tools and features available on the major social networking platforms. It is our aim to work with government to help propagate the messages there about the availability of tools and systems to help enhance child safety online.

Appendix 2 contains a draft outline version of a matrix which we hope to propagate under a single address link (in conjunction with the DBCDE) to be made available online for the benefit of all schools, parents, and children.

The IIA is also a member of the Safer Internet Group.[12] This new collective promotes a safer online experience for Australian families. It represents a broad alliance of both community and industry organisations looking to propose alternative measures to mandatory ISP filtering.

[11] See the Code at http://www.iia.net.au/images/content_services_code_registration_version_1.0.pdf

[12] (http://www.saferinternetgroup.org/).

OBSERVATIONS ON THE ROLE OF FILTERS

Technology can certainly augment the role of adult supervision. Many Australian families find filters a helpful adjunct to adult supervision.

As demonstrated by our work in this area, the IIA obviously supports the use of optional filters to help protect children from unwanted or inappropriate material. The Family Friendly Filter scheme evidences the range of products offered by security vendors. These products and services can be tailored for homes and schools as needed.

However, while many families and schools find filters useful, they are not to be seen as a substitute for parental guidance or well-founded education programs.

This conclusion is supported by findings of the OSTWG (at p. 23):

> As for filtering as a safety measure, there is a growing discussion about its use and effectiveness in the US and overseas. In the UK, government education watchdog Ofsted released a report this past February that rated 5 of 37 schools "outstanding" in online-safety provisions. The five "all used 'managed' systems to help pupils to become safe and responsible users of new technologies. 'Managed' systems have fewer inaccessible sites than 'locked down' systems and so require pupils to take responsibility themselves for using new technologies safely," Ofsted reported. The schools that used the stricter "locked down" filtering systems "kept their pupils safe while in school," the agency added, but "such systems were less effective in helping them to learn how to use new technologies safely."

While tools ranging from content filters to anti-malware programs have their place, they are no substitute for the lifelong protection provided by critical thinking. The best "filter" is not the one that runs on a device but the "software" that runs in our heads." (at p. 32).

THE MERITS OF ESTABLISHING AN ONLINE OMBUDSMAN TO INVESTIGATE, ADVOCATE AND ACT ON CYBER-SAFETY ISSUES

The IIA notes that the Committee is keen to receive comments on this reference with the view to addressing some tragic and terrible examples of misuse of social networks in the past.

Most popular social websites already have such services within their networks. These are outlined in our appendix and are designed to ensure that informed users do have the ability to draw on such resources when required.

At present, understanding and appreciation of such resources is uneven. In conjunction with the Government, schools and the community, the IIA proposes improved education on such facilities.

The IIA understands the case for an Online Ombudsman is inspired in part on the effectiveness of our local telecommunications, banking, insurance and other utility ombudsman-like offices.

In principle, they often operate as a "last resort" grievance service. This means that if a user complains to an ombudsman before taking their complaint to the service that caused the issue in the first place, they may only waste time getting their complaint processed. In other words, an Ombudsman may add another layer of regulation which may slow the response time for legitimate complaints to be dealt with by relevant providers.

We note that law enforcement agencies have generally praised the responsiveness under existing informal protocols with the main social media sites. We would not like to see anything undermine or add complexity to those arrangements. There is no evidence of systemic failure such as to warrant the establishment of such an office.

In addition where a jurisdiction crosses borders there is a risk that an Online Ombudsman may offer only symbolic assurance as they may not have any powers beyond that of publicity where a complaint is well-founded.

In the light of these concerns, the IIA remains to be convinced of the worth of establishing an Online Ombudsman.

RECOMMENDATIONS

Consistent with the points raised in this submission the IIA recommends the following actions for consideration by the Committee:

Recommendation 1

That the Government continue to sponsor and encourage research into the nature and extent of risk by minors online to identify the nature of the problems and where intervention is required. In particular, in view of the timeliness of this research and the clear advantages in having a comparative base with which to assess the relative position of Australian children online vis-a-vis their counterparts in 25 other nations, the Committee should urge Government funding for a parallel study in Australia to be undertaken.

Recommendation 2

That the Committee endorse a new approach by Government that promotes education, empowerment and law enforcement efforts to address cyber safety.

Recommendation 3

That the Committee insist on a more consistent and effective approach to resourcing cyber safety education programs that rely on clear goals, theory, interactive learning or integrates with school curricula. At the same time, these programs should avoid less effective techniques such as lectures, mere knowledge building or fear tactics. Ultimately, behavioural change should be our shared goal – a safer online experience requires children themselves to exercise informed and safer choices in their online activities.

Recommendation 4

That the Committee find against the proposal for the establishment of an Online Ombudsman until it can be established that such a role will add value to online safety and avoid adding delay to current processes

We are happy to provide the Committee with further information should it be required.

Peter Coroneos
Chief Executive, IIA
PO Box 3986 Manuka ACT 2603
ph: 02 6232 6900

Appendix 1 IIA Family Friendly ISP Program

ISPs who are compliant with the IIA Codes are eligible to apply for **IIA 'Family Friendly ISP'** status. This does not require joining the IIA, although IIA *member* ISPs are able to participate in the program at no cost. Family Friendly ISPs are authorised to display the Ladybird Logo which signifies adherence to best practice standards.

Presently ISPs representing about 85% of the market are IIA family friendly. We encourage all ISPs to support this program.

ISPs need to be aware that the IIA Codes exist as part of Australia's co-regulatory regime. This means that they are legally enforceable by the regulator, ACMA.

ISP Obligations
Under the registered Codes of practice, ISPs who provide access to users within Australia are required to:

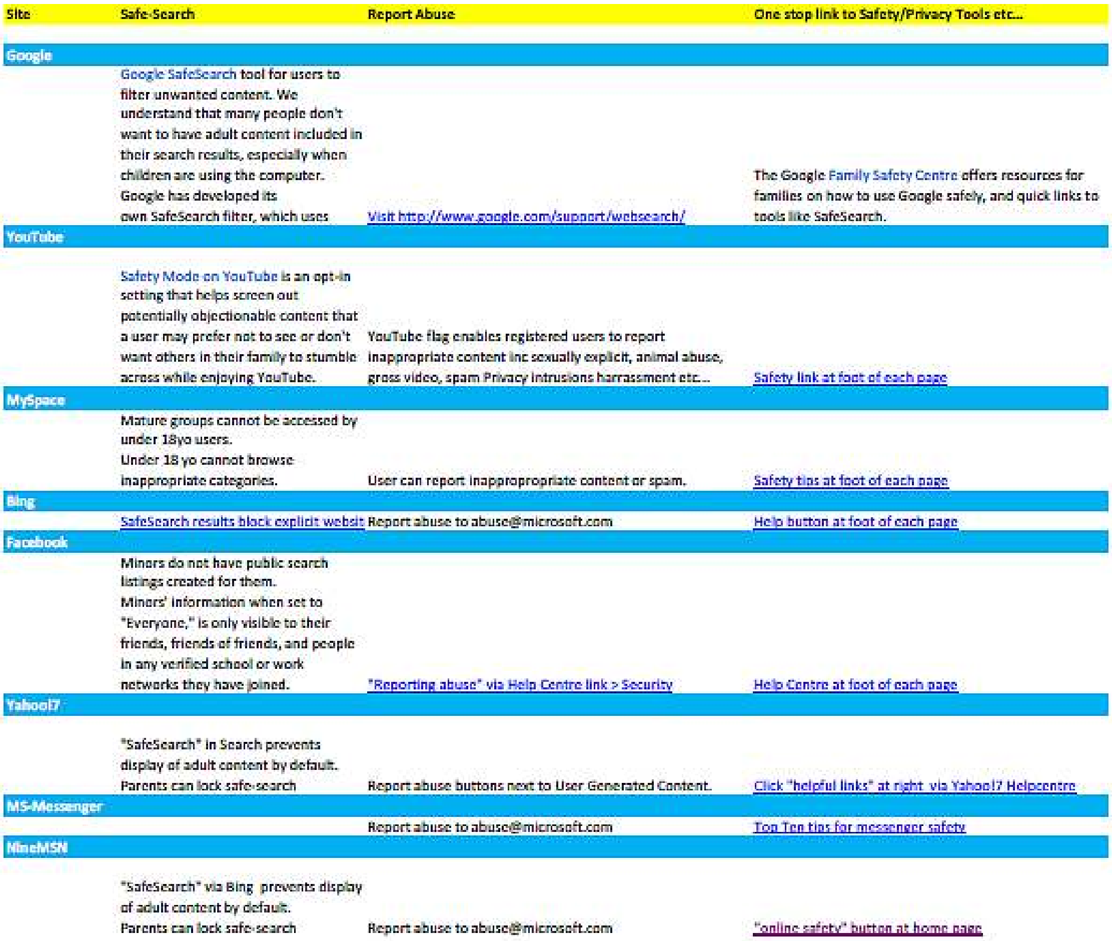
- take reasonable steps to ensure that Internet access accounts are not provided to persons under the age of 18 years without the consent of a parent, teacher or other responsible adult. A number of suggested options for achieving this are included in the Code.
- take reasonable steps to encourage *commercial* content providers to use appropriate labelling systems and to inform them of their legal responsibilities in regard to the content they publish. The IIA has compiled a resource for this purpose and ISPs are advised to simply direct users to the URL IIA Guide for Internet Users
- provide an optional filter or filtered service to users on a cost recovery basis.
- take reasonable steps to provide users with information about:
  - supervising and controlling children's access to Internet content
  - procedures which parents can implement to control children's access to Internet content
  - their right to make complaints to the ABA about online content
  - procedures by which such complaints can be made

The IIA has compiled a resource for this purpose - ISPs are advised to direct users to the URL IIA Guide for Internet Users.

For more information about the Family Friendly ISP scheme, please visit our site or contact the IIA on (02) 6232 6900.

Appendix 2: User Empowerment Resources for Social Media Sites

This is the first (summary) page of the matrix. The matrix continues with detailed information about each site's safety measures. DBCDE is working with the IIA to translate this into a layered, hyperlinked online version which can give situational advice to those accessing the online safety information provided by the Government.



Site	Safe-Search	Report Abuse	One stop link to Safety/Privacy Tools etc...
Google			
	Google SafeSearch tool for users to filter unwanted content. We understand that many people don't want to have adult content included in their search results, especially when children are using the computer. Google has developed its own SafeSearch filter, which uses	Visit http://www.google.com/support/websearch/	The Google Family Safety Centre offers resources for families on how to use Google safely, and quick links to tools like SafeSearch.
YouTube			
	Safety Mode on YouTube 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.	YouTube flag enables registered users to report inappropriate content inc sexually explicit, animal abuse, gross video, spam Privacy intrusions harrassment etc...	Safety link at foot of each page
MySpace			
	Mature groups cannot be accessed by under 18yo users. Under 18 yo cannot browse inappropriate categories.	User can report inapproproprlate content or spam.	Safety tips at foot of each page
Bing			
	SafeSearch results block explicit websit	Report abuse to abuse@microsoft.com	Help button at foot of each page
Facebook			
	Minors do not have public search listings created for them. Minors' information when set to "Everyone," is only visible to their friends, friends of friends, and people in any verified school or work networks they have joined.	"Reporting abuse" via Help Centre link > Security	Help Centre at foot of each page
Yahoo!7			
	"SafeSearch" in Search prevents display of adult content by default. Parents can lock safe-search	Report abuse buttons next to User Generated Content.	Click "helpful links" at right via Yahoo!7 Helpcentre
MS-Messenger			
		Report abuse to abuse@microsoft.com	Top Ten tips for messenger safety
NineMSN			
	"SafeSearch" via Bing prevents display of adult content by default. Parents can lock safe-search	Report abuse to abuse@microsoft.com	"online safety" button at home page

Appendix 3: Membership of the Internet Industry Association as at July 2010

AAPT

AARNet Pty Ltd

Accentu8 Marketing

Addisons Lawyers

AIMIA (Australian Interactive Multimedia Industry Association)

Always Online Pty Ltd

AMTA

APEX Internet (Ovee Pty Ltd)

ArcSight Australia/New Zealand

Armadillo interNET

AusCert (Uni of QLD)

Austar

Australian Association of National Advertisers

Australian News Channel Pty Ltd

Baker & Mckenzie

BarNetwork

BEST Internet & Telecom Pty Ltd

Bevenco

Brilliant Digital Entertainment Pty Ltd

CAIP (Canadian Association of Internet Providers)

CBIT Pty Ltd

Chalkport Pty Ltd

Clayton Utz

Cleartext Pty Ltd

Cogentis Pty Ltd

CommandHub Inc

ConnectingUp Australia

ContentKeeper Technologies

CouchCreative

Crime Stoppers Australia

Curtin University of Technology

CyberSecure Pty Ltd

D-LINK Australia Pty Ltd

depressioNet

Digital Marketing Institute

DirectoryAustralia.com

Dominet Digital Corporati

Dreamtilt

E-Vision Internet Pty Ltd

eBay Australia & New Zealand

eCorner Pty Ltd

Encassa Pty Ltd

Enex

Ericsson Australia

ETI Software

EuroISPA

F Secure

Facebook Inc,

Freehills

Gilbert + Tobin Lawyers

Gizmo

Google Australia Pty Ltd

Graham Bassett Barrister-at-Law

Grapevine Ventures

Griffith Hack

Henry Davis York

Highway 1 (Aust) Pty Ltd

Hive Empire Credit Card Finder and Balance Transfer Card

iiNet Limited

Interactive Games & Entertainment Association (IGEA)

Internet Society of China

InternetSafety.com

Internode Systems Pty ltd

iSeek

JRH Consulting

Kay Web Holdings

LawLive Pty Ltd

Leigh Adams Lawyers

Mackellar Insurance Brokers

Mama Wear

McAfee Australia Pty Ltd

Mercury Management System Services

Michael Johnson & Associates

Microsoft Australia Pty Ltd

Montimedia Communications

Myspace (Fox Interactive Media)

Netbox Blue

ninemsn

Nominum Inc

Northern Territory Library

Norton Rose

Odigo Media Pty Ltd

OPTENET S.A

Optus

OrderPoint Australia Pty Ltd

Orion Enterprise Buisness Solutions Pty Ltd

Ourbrisbane.com

Outpost24 Australia

Paul Budde Communications Pty Ltd

Pipe Networks Pty Ltd

Port of Brisbane Corporation

PPS Internet/Studentnet

QK

Queensland University of Technology (QUT)

Rackspace

Redlaunch Pty Ltd

Rentbook Pty Ltd

Revium Pty Ltd

Rural Systems (Eyre OnLine.com)

SABRENet Ltd

SAGE-AU

Save My Musik

Search IQ Pty Ltd

Shifted Pixels

Softel Systems Pty Ltd

Sophos

Sportal Australia

SSI Pacific Pty Ltd

STRATSEC.NET PTY LTD

Summit Internet Solutions

Sustainable School Shop

Symantec Australia

Tech2home

Telstra Corporation

The Eros Association

thinkgroup Pty Ltd

ThreatMETRIX

Trade Live Pty Ltd

Trend Micro Australia

Truman Hoyle Lawyers

TrustDefender

Universities Australia

University of Adelaide

University of Queensland (UQconnect)

Unwired Australia

UpdateTime.com Pty Limited

USIIA

Verizon Business

Virgin Mobile Australia

Vision Australia

Vodafone Hutchison Australia

WAIA (Western Australian Internet Association)

Watchdog International Ltd

Web Management Interactive Technologies

Webroot Software Pty Ltd

Wontok Enterprises Pty Ltd

X|Media|Labs (aka Cross Media Labs)

Yahoo Search Marketing