Submission

on

Cyber-Safety

to the

Joint Select Committee on Cyber-Safety

Department of House of Representatives
PO Box 6021
Parliament House
Canberra ACT 2600
Telephone: 02 6277 4202
Facsimile: 02 6277 2219
Email: jscc@aph.gov.au
Website: www.aph.gov.au/house/committee/jscc/

by

FamilyVoice Australia

4th Floor, 68 Grenfell St, Adelaide SA 5000
Telephone: 1300 365 965
Facsimile: 08 8223 5850
Email: office@fava.org.au
Website: www.fava.org.au

20 June 2010

TABLE OF CONTENTS

1. Introduction

The Joint Select Committee on Cyber-Safety has been established following resolutions of the House of Representatives and the Senate.

On 13 May 2010, the Committee resolved to focus initially on the following topics as they relate to children and young people:

- the online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles);
- abuse of children online, particularly cyber-bullying;
- inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of eating disorders, drug usage, underage drinking, smoking and gambling);
- identity theft;
- breaches of privacy;
- Australian and international responses to these cyber-safety threats;
- opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with these cyber-safety issues;
- ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying; and
- the role of parents, families, carers and the community.

Submissions from the public on these topics and any other matter in the terms of reference have been invited and are to be received by 25 June 2010.

Additional matters in the terms of reference include:

- the nature, prevalence, implications of and level of risk associated with exposure to illegal and inappropriate content;
- the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues.

This submission will address general principles of cyber-safety; inappropriate social and health behaviours in an online environment; and the nature, prevalence, implications of and level of risk associated with exposure to illegal and inappropriate content.

2. General principles of cyber-safety

The rapid developments in information and communications technology over the past decades can create a sense that there has been a radical change in the way we live.

However, despite both utopian and dystopian visions of the impact of such technological change, it remains true that fundamental human nature has not been altered.

As the great Russian write Alexander Solzhenitsyn observed:

> *Gradually it was disclosed to me that the line separating good and evil passes not through states, nor between classes, nor between political parties either, but right through every human heart, and through all human hearts. This line shifts. Inside us, it oscillates with the years. Even within hearts overwhelmed by evil, one small bridgehead of good is retained; and even in the best of all hearts, there remains a small corner of evil.*[1]

All the participants in the cyber-world are human beings and therefore capable of using the new technologies for good – or for evil.

The cyber-world therefore cannot be exempt from the kinds of measures necessary in all areas of human communities to protect members of the community – and most especially the weak and vulnerable, including children – from the evil that others may do.

Bearing these things in mind, the following principles are offered as a framework for policy making on cyber-safety:

- The basic principles of law should apply to exchanges in the cyber-world in the same way as they apply to human communities in general. This applies to principles of criminal law, contract law, defamation, privacy law, censorship and classification law and so forth.

- The nature of the cyber-world may require specific applications of the general principles to ensure that they are effectively applied in this context.

3. Inappropriate health and social behaviours

The terms of reference mention some specific inappropriate health and social behaviours which may be fostered or facilitated by cyber-technology.

These include technology addiction, online promotion of eating disorders, drug usage, underage drinking, smoking and gambling. This list could be expanded to include pornography addiction, suicide promotion, sale of unregulated pharmaceuticals and financial fraud.

Outside the cyber-world the law protects Australians in various ways from these harms.

Legal measures include prohibitions on the sale of illicit drugs and unregulated pharmaceuticals; material that is or would be "Refused Classification"; restrictions on advertising of alcohol and tobacco products; prohibition on the promotion of suicide or instruction in the methods of suicide; penalties for fraudulent schemes; and regulation and licensing of gambling.

Many of the harms being targeted require a law with domestic effect that is complemented by customs law, or other laws which take into account the fact that Australia is part of a world where other countries may not share our values or may have less effective law enforcement.

In seeking to ensure that the basic principles of law relating to these harms apply in the cyber-world, it is important to address foreign as well as domestic sources of harm.

Just as our laws against illicit drugs include strong customs measures as well as laws prohibiting drug trafficking within Australia, so laws are needed to address harms which originate from outside Australia in the cyber-world.

An example is the need for more effective laws against promoting or instructing in methods of suicide.

3.1 Suicide promotion and instruction

Australian law prohibits the use of any carriage service (including the internet) to "directly or indirectly counsel or incite committing or attempting to commit suicide" or to "promote a particular method of committing suicide; or to provide instruction on a particular method of committing suicide".[2]

However, in the absence of a mandatory filtering scheme, these provisions have proved ineffective in preventing suicides following instruction and encouragement received by vulnerable people over the internet.

In April 2007, two 16 year old girls, Jodie Gater and Stephanie Gestier, committed suicide. They hanged themselves from the branch of a tree a few kilometres from their homes in Melbourne's Dandenong Ranges.[3]

It was later discovered that the children had followed step-by-step instructions from a suicide website hosted in the Netherlands.[4]

The site offered practical and illustrated advice on a variety of methods including strangulation, asphyxiation and poisoning.

Liam Bartlett of Channel Nine's *Sixty Minutes* program reported Rob Gater's horror when he discovered that his daughter and her friend had used the internet to find a virtual suicide manual - telling them the kind of rope and knots to use, plus other deadly details.[5]

Similar incidents have occurred in Britain.

In 2008 it was reported that up to 29 "internet suicides" had been identified as having occurred in Britain since 2001, including a cluster of suicides of young people in the Welsh town of Bridgend. Various suicide promoting websites had been implicated, including one sponsored by California-based Nagasiva Yronwode. Yronwode identifies as a Satanist and runs the so-called Church of Euthanasia, which advocates suicide as a means of saving the world from overpopulation.

Another website sponsored by Dutch woman Karin Spaink gives detailed instruction in 41 methods of suicide. A Swedish man, Calle Dybedahl, who also hosts a suicide instruction site, claims that death is not an inherently bad thing.[6]

Dr Phillip Nitschke, Australia's best known promoter of euthanasia, believes that the means and knowledge of how to commit suicide should be available to every person. During an interview in 2001 he said:

> *I do not believe that telling people they have a right to life while denying them the means, manner, or information necessary for them to give this life away has any ethical consistency.*
>
> *So all people qualify, not just those with the training, knowledge, or resources to find out how to 'give away' their life. And someone needs to provide this knowledge, training, or recourse necessary to anyone who wants it, including the depressed, the elderly bereaved, [and] the troubled teen. If we are to remain consistent and we believe that the individual has the right to dispose of their life, we should not erect artificial barriers in the way of sub-groups who don't meet our criteria.* [7]

Dr Nitschke's webite, located offshore, offers his *Peaceful Pill Handbook* for sale.[8] This book was prohibited from sale or distribution in Australia in 2007 after it was Refused Classification for instructing in crime, including the manufacture and importing of illicit drugs (barbiturates) as well as in how to avoid a coronial inquiry following an assisted suicide.[9]

Dr Nitschke recently announced that Exit International would be offering mail order deliveries of a solid version of Nembutal, a lethal substance, which could be reconstituted as a liquid for consumption.[10]

These developments point to the urgent need for implementation of the Rudd government's proposal for a mandatory national filtering scheme that would prevent, or at least significantly hamper, access to sites containing material that would be Refused Classification. Suicide promotion and instruction sites such as those implicated in the suicides of young people in Victoria and in Britain, as well as the website of Exit International, should be blocked from easy access by anyone using the internet in Australia.

Recommendation 1:

Suicide related material, as defined in Section 474.29A of the Criminal Code, should be included as prohibited material in the proposed scheme for mandatory filtering of the internet.

3.2 Gambling

After discussing the evidence that suggests a high prevalence of problem gambling among online gamblers, the Productivity Commission's draft report concludes:

> *While the risks associated with online gambling are likely to be overstated, the relatively high prevalence of problem gamblers is still a cause for concern. At the very least, it indicates that the internet is very attractive to this group and, though the evidence is weak, gambling online may exacerbate already hazardous behaviour. In any case, it is clear that careful regulation of the industry is warranted.*[11]

The *Interactive Gambling Act 2001* prohibits the establishment of online gaming services on Australian-hosted internet sites.

The draft report correctly points out that this prohibition fails to prevent Australians, including problem gamblers, accessing online gaming service hosted on internet sites located outside Australia.

The draft report proposes the repeal of the *Interactive Gambling Act 2001* and the introduction of regulated online gaming services in Australia.

The reasoning is faulty. Even though regulated online gaming services may lead to somewhat less problem gambling than unregulated offshore online gaming services, it is unclear how the existence of regulated Australian gaming services will necessarily draw problem gamblers away from offshore unregulated online gaming services.

Moreover, the introduction of regulated Australian-based online gaming services is likely to attract more gamblers overall to use online gambling. Australian sites could potentially increase the total participation in gambling of all kinds in Australia. Even though regulations and harm minimisation measures may be put in place for Australian-based online gaming services, an expansion in the availability of gambling is nevertheless likely to lead to at least some increase in the prevalence of problem gambling.

Curiously, the draft report does not even consider whether the *Interactive Gambling Act 2001* could be expanded to require internet service providers (ISPs) to take effective measures to block all identified online gaming services located outside Australia in order to prevent Australian consumers from readily accessing such sites.

The Rudd government has a commitment to introducing a national mandatory scheme for filtering access to overseas sites that contain material that would be Refused Classification under the national classification scheme. This includes child pornography, violent pornography, terrorist promoting-material and suicide promotion and instruction.

It would make sense to include online gaming sites in this filtering scheme.

Recommendation 2:

Access to offshore online gaming sites should be made more difficult by including them in the proposed national mandatory filtering scheme.

4. Inappropriate material

The National Classification Scheme currently applies to publications, films and computer games.

It is a cooperative scheme involving the Commonwealth, States and Territories.

The scheme includes advisory categories (such as G, PG and M for films and computer games) and age restricted categories (such as Restricted Category 1 and Restricted Category 2 for publications; MA15+ for films and computer games; and R18+ for films).

Additionally, X18+ films may only be sold in the Australian Capital Territory and in parts of the Northern Territory that are not affected by the Northern Territory Emergency Response (NTER) provisions.

Material which, for various reasons, exceeds the highest classification in each medium is classified Refused Classification (RC).

The current law provides for takedown notices for material hosted in Australia that is or would be Refused Classification, or which is or would be classified as MA15+, R18+ or X18+ but which lacks an effective age verification system.

Under a complaints-based system, if such material is hosted offshore, the relevant URLs are added to a "black list" maintained by the Australian Communications and Media Authority (ACMA). This black list must be used by filter services that are approved to offer opt-in filtering to block the listed URLs for end users.

The Rudd government was elected with a promise to further investigate and, if feasible, introduce a national mandatory filtering scheme. Under this scheme, all ISPs would be required to block a new ACMA-managed black list which would consist of URLs for pages containing Refused Classification material. After investigations have confirmed the feasibility of such a scheme, the government has confirmed its intention to introduce legislation for such a scheme.[12]

This proposal is consistent with the general principles for policy making on cyber-safety enunciated above.

Opponents of the scheme commonly put forward several arguments including:

- *The scheme would degrade internet performance.*

The evaluation by Enex Testlabs indicates that the scheme could be implemented effectively with minimal degradation of internet performance.[13]

- *The scheme is a violation of the right to freedom of access to information.*

This is really an argument for no censorship at all in any medium, not even censorship of extreme child abuse material, or films of real rape and murder. There has never been an absolute right to freedom of access to information. This right has always been qualified by the need to protect the community, and there is no logical reason why the internet should be treated differently from newspapers, films, radio or television.

Those who jammed Australian Parliament House and federal government websites with a cyber attack in February 2010, demanding unrestricted access to pornography, merely demonstrated their immature, selfish disregard for the rights of others.[14]

- *The scheme is likely to lead to suppression of political views contrary to those of the government such as happens in China.*

China is a one-party state with no democratic elections. An Australian filtering scheme requires legislation which needs to be debated in our multi-party democratically elected parliament. The implementation of the scheme will be subject to scrutiny by members of parliament (through means such as parliamentary questions and estimates committees) and the media.

- *The scheme will not succeed in completely blocking access to blacklisted URLs as there are various technological means of circumventing filtering.*

This is also true for laws prohibiting the import and distribution of offensive material. Customs officers cannot open every package. However, laws which are efficiently enforced can contribute to a significant reduction in access to offensive material. This is a worthwhile goal, even if complete elimination of access is never achieved.

Recommendation 3:

Legislation for the mandatory filtering scheme should be introduced as soon as possible and should be supported by all members and senators.

4.1 Improving the proposed scheme

The mandatory filtering scheme, as currently proposed by the government, could be enhanced in several ways to improve cyber-safety. Some of these improvements could be included in the initial implementation of the scheme. Others could be made once the scheme has been running successfully for a period of time.

- Categories to be filtered should include not just Refused Classification but other categories where the law already prohibits hosting of material in Australia. This includes material which promotes, encourages or instructs in methods of suicide; online gaming sites; and sites facilitating financial fraud.

- Senator Conroy's media release of 15 December 2009 stated that: "*The Minister for Home Affairs yesterday announced a public consultation process into whether there should be an R18+ classification category for computer games. Until this process is complete, online computer*

games will be excluded from mandatory filtering of RC content." On 7 May 2010 the Minister for Home Affairs announced that the Standing Committee of Censorship Ministers had requested "further analysis of community and expert views" on the proposal for an R18+ classification for computer games.[15] This process could take quite some time before any final decision is made. In the meantime the government's position means that games which, even if an R18+ classification were introduced, would still be Refused Classification, would not be filtered. One example is the Japanese computer game *RapeLay*, which includes rape of children. It would be better for computer games which would be Refused Classification under current Australian law to be filtered. In the event of the law being changed to provide for an R18+ classification for computer games, then the URLs of any games subsequently reclassified R18+ could readily be removed from the filter blacklist.

- The Rudd government's scheme will encourage service providers to offer further family-friendly filtering through a grants scheme. Standard ISP service could be required to be filtered to exclude MA15+, R18+ and X18+ level material. MA15+ and R18+ material could be made available only on an opt-in basis with appropriate age verification.

- X18+ material should be excluded. It is banned from sale by all six States and, because of its known use in contributing to child abuse, has recently been banned in parts of the Northern Territory.

- The blacklist of URLs should not just be compiled by complaints and the supply of lists of child abuse sites from overseas enforcement agencies. A tender should be let for a pro-active web crawler based system that actively seeks out URLs which contain prohibited material.

- Real time filtering could be added as this technology becomes more efficient.

Recommendation 4:

The legislation to implement the filtering scheme should include, in the material to be added to the black list, material which promotes, encourages or instructs in methods of suicide, online gaming and fraud schemes. Computer games which have been or would be Refused Classification under current Australian law should also be included on the black list.

Consideration should be given to future enhancements to the scheme to make the default filtered ISP service family-friendly, by filtering all MA15+, R18+ and X18+ material. MA15+ and R18+ material should be available on an opt-in basis with appropriate age verification. X18+ material should be prohibited, as it is prohibited under the laws of all six states as well as under the NTER provisions in parts of the Northern Territory.

The method of compiling the black list should be continually improved with the use of proactive approaches such as web crawlers used when feasible. Real time filtering should be considered as it becomes more efficient.

5. Conclusion

Special interest groups are likely to engage in special pleading that the cyber-world is so different than the rest of the world that different rules should apply. This special pleading should be rejected. Despite the rapid developments in technology, the cyber-world still involves real human beings who are capable of inflicting harm on others as well as doing good. Law is designed to restrain evil actions. It must apply to the cyber-world on the same basis as it does in other spheres of human

interaction. Specific applications of the law may be necessary to ensure their effectiveness in the cyber-world.

The government's proposed national mandatory filtering scheme is an important contribution to achieving cyber-safety. It should be supported by all members and senators. It should be improved as proposed in the recommendations in this submission.

6. Endnotes

---

1. Solzhenitsyn, A. *The Gulag Archipelago 1918-1956*, London: Collins & Harvill Press, 1975, [Vol. 2], p 615.

2. *Criminal Code Act 1995,* Schedule, Section 474.29A.

3. "Death pact teen's grim poems", *Sydney Morning Herald* , 23 April 2007; http://www.smh.com.au/news/national/grieving-mother-asks-why/2007/04/23/1177180529637.html

4. Carr-Gregg, M. and McLean, S., "Black holes in net space", *Herald Sun*, 23 May 2007; http://www.heraldsun.com.au/opinion/black-holes-in-net-space/story-e6frfifo-1111113591392

5. "Web of darkness", *Sixty Minutes*, Channel Nine, 17 May 2007; http://sixtyminutes.ninemsn.com.au/stories/liambartlett/267889/web-of-darkness

6. Sawer, P., "Predators tell children how to kill themselves", *Daily Telegraph*, 17 February 2008; http://www.telegraph.co.uk/core/Content/displayPrintable.jhtml;jsessionid=HZG5IYACS003PQFIQMGSFF4AVCBQWIV0?xml=/news/2008/02/17/nweb117.xml&site=5&page=0

7. Lopez, K., "Euthanasia Sets Sail : An interview with Philip Nitschke, the other "Dr. Death.", *National Review Online*, 5 June 2001; http://www.nationalreview.com/interrogatory/interrogatory060501.shtml

8. http://www.exitinternational.net/

9. Classification Review Board, *The Peaceful Pill Handbook : Reasons for Decision,* 24 February 2007.

10 Humphry, D., "Dr Nitschke says he'll be selling Nembutal pill next year", *Assisted Suicide Blog*, 30 October 2009; http://assistedsuicide.org/blog/2009/10/30/dr-nitschke-says-hell-be-selling-nembutal-pill-next-year/

11. *Gambling: Productivity Commission draft report,* October 2009, p 12.15; http://www.pc.gov.au/__data/assets/pdf_file/0010/91882/gambling-draft.pdf

12. Conroy, S., *Measures to improve safety of the internet for families*, 15 December 2009; http://www.minister.dbcde.gov.au/media/media_releases/2009/115

13. Enex Testlab, *Internet Service Provider (ISP) Content Filtering Pilot Repor*t, 2009; http://www.dbcde.gov.au/__data/assets/pdf_file/0004/123862/Enex_Testlab_report_into_ISP-level_filtering_-_Full_report_-_Low_res.pdf

14. *The Sydney Morning Herald*, 10 February 2010; http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-websites-20100210-nqku.html .

15. O'Connor, B., *R18+ Classification for Computer Games Consultation Report Released*, 7 May 2010; http://www.ministerhomeaffairs.gov.au/www/ministers/oconnor.nsf/Page/MediaReleases_2010_SecondQuarter_7May2010-R18+ClassificationforComputerGamesConsultationReportReleased