SUBMISSION No. 105

INTRODUCTION

My name is Geordie Guy. I am a Sydney based technology expert and an active member of several organisations and communities which are recognisable in technology policy in Australia. Rather than lead a submission to the committee from any of those organisations or communities I've chosen to make an individual submission.

Technology policy in Australia is almost uniquely a freefall into confusion, conflicts of interest (and the opportunities for more conflicts of interest), moral crusading, uninformed decision making and fiction perceived as reality. The committee has the opportunity to address these problems, and we as Australians an opportunity to address the committee. My submission is accompanied with my sincerest hope that the members of the committee are able to provide leadership to the parliament of Australia and arrest this freefall, and perhaps point out the start of a path into a rational, civil and confident Australia online.

THE ONLINE ENVIRONMENT IN WHICH AUSTRALIAN CHILDREN CURRENTLY ENGAGE

The committee is to inquire into and report on, how children access technology and who in the community has "buy in" on those methods, for example whether government, children, parents or the digital economy itself is relevant (and in what ways) to how children use the Internet.

How this came to be an issue under the terms of reference of the committee is confusing to say the least, because there could hardly be said to be a less relevant issue in Australia's digital landscape, particularly to the children in question.

The methods in which children gain access to online Australia and the online world is analogous to a home's electricity supply in at least two key ways. Firstly, children have no interest whatsoever in the machinations of how electricity comes to their household, whether it is AC or DC, 240 volts or 110. Unless it's at least peripherally related to something they *are* interested in, perhaps whether it's derived from environmentally sustainably sources, children simply accept (indeed, expect) a readily available supply of electricity and the same is true for access to our online world. The second way in which access to the online environment is the same as electricity, is that children necessarily choose the shortest path to what they want in the same manner as electricity follows "the path of least resistance". If a teacher, librarian or parent interferes with one method of access to the sense of community that children seek with each other, it is no longer the easiest way in which to talk about the day's events, gossip about relationships that are forming within the peer group or seek assistance with life's problems and that child will simply switch from SMS to instant messaging, or from instant messaging to using a social networking website's chat feature. Children could not care less about how they access communities digitally, they simply do so in the way that is most simple or intuitive to them and if that way becomes less simple or intuitive due to the interference of the offline community, they switch.

The only thing that may see a child continue with their chosen method of communication and access to information in the face of interference is if the child is able to erect some sort of privacy protection. Members of the committee may be familiar with offline versions such as a note passed in class that reads "⊐□□> ⊐□ ⌋⊏>□⌜ ⌊⌊⌋VV"[1] or pig Latin. Online methods of protecting privacy do exist. They are not flawless; they're not even very good, because they are only intended to make it more complicated for those who would interfere. If they don't work, they are abandoned because the point is not the access method or who is a gatekeeper; the point is simply the community.

So what is the harm in the committee investigating these things in detail? If the means truly has no bearing on the end, what harm could we do?

In 1944 the German army made use of what would be a very dangerous weapon called the "V1". This bomb was a 25 foot long precursor to the modern day cruise missile and was followed by other classes of weapon that were deployed from Germany or controlled areas, into London itself against civilians. One of the most regrettable wastes of time and money throughout the whole of the Second World War was a committee tasked with predicting where these weapons would strike by collecting and examining information about previous strikes. Of course the strikes were *random*. Even were the German army to attempt to target the weapons to particular areas, environmental factors as well as this new technology that only scarcely made the weapons possible meant that the strikes were as much of a surprise to the Germans as the English. Apophenia, the human tendency to think we can see patterns in random or at least unrelated data, meant that the English attempted to predict the unpredictable instead of concentrating on a broad safety plan that could've dealt with all contingencies.

The committee should not attempt to establish patterns in broadly irrelevant precursors to online interactions, advising instead that if there *are* discernible threats to children online that don't exist offline, that they be dealt with in a holistic manner.

[1] "meet me after class" rendered in pigpen, a common "schoolyard cipher" which has been in use for approximately 300 years.

THE NATURE, PREVALENCE, IMPLICATIONS OF AND LEVEL OF RISK ASSOCIATED WITH CYBER-SAFETY THREATS, SUCH AS:

Before I investigate the cybersafety threats, it's important to understand what we mean by cyber-safety.

Cyber-safety or cybersafety is a made up term, or a "neologism". The term doesn't appear readily outside of Australia[2], and in particular it is native to the Australian government, child protection agencies which have a close relationship with the government (such as Brave Hearts who have had several governmental advisory body cameos) and organisations seeking to commercially supply solutions to the perceived problem. This isn't unusual, the Australian government writes far more contemporary lexicon than it reads, coming up with terms like "ICT" to mean what the digital economy describes as "IT" or "technology", terms which are foreign to mainstream Australia and the digital economy itself.

If one uses Google's search suggestion feature to provide associated terms that fit with cyber-safety, "ACMA" is the highest ranked – suggesting that an Australian government statutory body tasked with Internet regulation is the most popular phrase around the world to be associated with the term. This is not because Australia leads the orchestral swelling against a global online enemy, it's because we are a lone triangle player insisting our melody is groundbreaking.

In terms of amount of web pages returned as search results though Google, there are 189,000 results for "cyber safety"[3] as at the 5th of July 2010.

In order to provide a sense of perspective on the global prevalence this term and perhaps its associated risk, "toenail fell off" yields 239,000.

Let use be quite clear. There is no globally accepted term "cyber-safety". It is as Australian an invention as the humidicrib, but profoundly less relevant to the safety of young people.

When we understand that Australia is alone in grouping a list of ill-understood (but enthusiastically condemned) aspects of online and offline life under this umbrella term, we're ready to examine these issues which the committee has been told comprise it, and what their relevance to online Australia is.

[2] There are some examples of the term outside of Australia, but the presence of a kangaroo in San Diego Zoo is not evidence of the international prevalence of the animal

[3] This is the most prevalent rendering of the term, a handful of hits exist for the portmanteau of "cybersafety".

ABUSE OF CHILDREN ONLINE (CYBER-BULLYING, CYBER-STALKING AND SEXUAL GROOMING);

Cyber-bullying, if we take this to mean yet another application of "cyber" affixed to the front of any social ill or crime which has existed for hundreds or thousands of years; is the threatening, intimidation or harassment of a child as per any other definition, except the Internet forms part of the method used by the perpetrator to do so. Cyber-stalking is similarly a situation where hiding in the front hedge of a victim's abode is substituted for hiding in their email inbox.

With this established, setting aside any confusion we may have as to why these particular methods of bullying, stalking and harassment are deserving of joint select attention, we can look at if it they're prevalent and whether or not they're addressed.

To address the second question first, these activities are without question criminal offences.

Section 474.17 of the Commonwealth Crimes Act states;

Using a carriage service to menace, harass or cause offence

(1) A person is guilty of an offence if:

(a) the person uses a carriage service; and

(b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

Elsewhere under Australian law, a carriage service is essentially defined as any service which uses electricity to communicate – covering both the telephone network and the Internet. This is unequivocal, and even were it to be confusing, the very act of making another person's life a misery is adequately covered under other state and commonwealth provisions such as S474.14[4] of the Crimes Act, and those which do not even mention (but do not exclude) the Internet as being part of the commission of a crime. In summary, it is unsurprisingly the case that being an offensive and reprehensible individual and engaging in the recreational menacing of another Australian is prohibited by law.

So does the criminal justice system deal with offenders? After all, it seems for all the areas that Australia lacks behind the rest of the world in reasoned, evidence based technology policy, we have at least one area in which we've not erroneously figured that because the Internet is involved it's a whole different ball game.

No. It doesn't seem so. In 2009 I was asked to comment for ABC Ballarat in my capacity as a board member of Electronic Frontiers Australia, on the website "Whozadog" (as in "who is a dog?"). The website's premise was as simple as it was disgusting, requiring users to register for an account in order to gain access to an

[4] The use of a telecommunications network to commit a "serious offence", which is taken to mean an offence which carries a penalty of five years or more. Stalking and threatening behaviour offences in the states typically carry a five year sentence.

online community explicitly for the purpose of menacing, harassing and causing offence to other members of either other members of the online group, or residents of Western Melbourne and greater Victoria. As part of the news report, ABC Ballarat contacted police who advised that there was no action they could take, because the equipment that allowed the website to be available, was located in the United States. The police believed they were being called upon to censor the website, not police the law regarding how Australians act towards each other.

This is just one example of many in Australia's multipart attitude to the behaviour of Australians, and how it is somehow considered different if we are using a computer. It is my opinion that every participant in the Whozadog website community likely had a case to answer under section 474.17 of the Crimes Act and given that it was an online forum to discuss offline individuals, that it would've been possible for the police to investigate who was potentially committing these offenses. I believe that when I have been called upon to provide comment on the establishment of various groups on the social networking site Facebook, that the participants are similarly likely to run afoul of the law. I believe that when a child uses a mobile phone or instant messaging client to harass another child because it allows for around-the-clock annoyance instead of having to wait to see their victim at school the next day, that it should not be considered the fault of technology which is rapidly becoming the most important enhancement in Australian life. It is my submission that Australian police and other regulatory bodies need to either admit that they do not understand the law if for some reason the circumstances of a case includes a computer, or advise that they are under-resourced, or advise that their discretion is being applied due to a lack of prevalence of these types of crimes, or that the risks have been deemed minimal and police resources are better focussed elsewhere.

The committee should advise that it is imperative that Australia stop attempting to find a suitable response distinction between crimes committed using technological means and those which are not. The committee should advise that the police have conflated their responsibility of public safety with a perceived public expectation that they act as censors (possibly due to a trend towards censorship as a safety response in Australian policy), and seek clarification for police responsibility. The committee should further examine extending reporting responsibilities in schools to include instances of criminal behaviour of a menacing or harassing nature online or offline.

Compared to the public sector's predilection for making up words for things it is frightened of online, sexual grooming is a term which is recognised more widely, but is only as applicable to the realities of online life.

Predation of children online is possibly the number one area for hysteria in those who don't fully comprehend how online life interacts with online life, and the focus of the arm flailing and hand-wringing appears to be, again, in the legislature. It is largely absent in a community which occasionally furrows its brow at 6:00pm tabloid television reports of millions of children annually being abused online, but then goes back to supervising their offspring's interactions in the online and offline community at a level commensurate with their age – perhaps commenting that the party is on a school night and asking who's supervising if the interaction is offline, and commenting that the child has been quiet on the computer and asking who they're talking to if the interaction is online.

These measures, adapted only slightly for whether a computer is involved, are an example worth celebrating because research submits that parents (and others in the community) applying a proportional response to the interactions children have online and off, appears to be a course of action grounded in fact. In a prominent latest example of parents proving they know what is better for their children than our bicameral parliament does, the research of Janis Wolak, David Finkelhor, Kimberly J. Mitchell and Michele L. Ybarra in *Online "Predators" and their Victims: Myths, Realities and Implications for Prevention and Treatment*[5], systematically dismantles the very notion that there is an online world of sexual misdemeanor by adults towards children that is meaningfully different to offline sexual offences.

The reality is, both presented in contemporary research and observable if we calm down enough to watch our surroundings, children are given to risk taking behavior. Some of them take sufficient risks either online or off, as to place themselves in danger (because risk and danger are not the same thing). Within this framework of risk taking behavior, some children will deliberately and knowingly seek inappropriate relationships with adults, or lack the social skills to resist the advances of an adult, or lack the social skills (or indeed the appropriate environment) to seek assistance from a peer or authority in dealing with the problem.

This cuts off the concept of "sexual grooming" at the ankles. There is demonstrably no evidence which simultaneously withstands scrutiny and suggests the existence of an Internet epidemic of adults preparing children for sexual relationships. There is of course evidence, as there has been forever, that adults seek inappropriate relationships with children and in some circumstances a child either does not successfully avoid the relationship or indeed seems to seek it. If we hope to help children develop strong, appropriate, healthful relationships with other children, then as they grow into young adults and adults, discover strong, appropriate and healthful relationships there, we must stop scouring the Internet for the proverbial dirty man in the trench coat.

[5] http://www.nsvrc.org/publications/articles/online-"predators"-and-their-victims-myths-realities-and-implications-preventi

The committee should recommend that increased funding and resources be provided to programs that educate children on what relationships are safe and happy ones, and what options are available in the event that an unsafe or unhappy relationship appears to be developing. The committee should advise against, and be wary of the uselessness of, any proposal which seeks to regulate the Internet further as an answer to these relationships (such as an "online ombudsman").

Exposure to Illegal and Inappropriate Content

Offline, cocaine is a substance which is evidence of an illegal activity (the production of illicit drugs). Further, most conceivable uses of it such as sale, consumption, driving under its influence etc. are illegal as well.

Cocaine is of course not illegal in and of itself, it is not illegal because *things* are not regulated by criminal law, rather *actions of people* are regulated and specifically in Australia the actions of Australians are considered illegal if deemed so by a court of law convened to decide the matter.

Impropriety offline is only marginally more complex. Of course crime is improper and inappropriate, but while burglary is considered inappropriate (to the extent that it is illegal), improper behavior is not necessarily illegal. Were I to belch loudly at a dinner party I may be asked to leave but I would be surprised if the police arrived to take action on the matter.

One needs no law degree to comprehend the scales involved in this issue, in fact a complete high school education is probably not required. Human behavior can be improper, in which case it is dealt with by whatever applicable social rules are in place for the situation, or may be so improper that it is illegal in which case it is dealt with by the law (in effect, merely a more formal applicable social rule).

All of this logic flies out the window when Australia considers the Internet, and regrettably only when Australia does it. In Australia we have the normal concepts of material online which is deemed inappropriate in which case it is avoided, or we have content which is cocaine-like and evidence of severe wrongdoing that warrants police attention. *However,* we also have a globally unique third category called "Refused Classification". Refused classification is in essence a strange sort purgatory between these two categories; it is more offensive than what we may perhaps actively seek (although this is not universally the case), but not offensive enough to warrant the attention of the police. It is that which exceeds the government's belief as to what we should be avoiding, but does not exceed the law – which is what we believe we should be required to avoid.

To understand what constitutes refused classification we must understand at the very least, three pieces of legal instrument. The first is the *Broadcasting Services Act 2001* which proudly declares the Internet a film by establishing its classification under the same rules and regulations as movies. The second is the *Classifications (Publications, Films and Computer Games) Act 1995* which outlines what the classifications are, and the *Guidelines for Classification of Films, Computer Games and Internet Content* are a set of examples of things described under the Classifications Act just in case the Australian Classification Board was at a loss for what jargon such as "illegal" or "sex" may mean.

The result of all this, is that we have a similar online classification and censorship regime such as what may be found on free to air TV (with the exclusion of SBS and ABC which are separately self-regulated), with classifications of G, PG, MA and so on describing age categories.

What has this to do with "RC"?

Put simply, anything online which cannot be classified as G, PG, M, MA, R or X as if it were a movie for a cinema to show, is refused classification and prohibited from sale or public display. It is not illegal to possess (with the exception of Western Australia and some parts of the Northern Territory), it's just a "D) - none of the above" category which is banished off the Internet by the Australian Communications and Media Authority if it is Australian hosted, or is proposed to be censored by ISPs at the requirement of the federal government if their ISP censorship[6] proposal goes ahead.

How does any content get in this pickle? Some of is unable to be rated G, PG, M, MA, R or X because it is evidence of a crime, but the majority of it is just "too gross" or unable to be rated due to weird anomalies in classification law. "Too gross" includes anything which has even a peripheral dealing with crime, violence or revolting or abhorrent phenomena in an "offensive manner" - a computer game which depicts graffiti is refused classification currently, as are the films Ken Park and Baise Moi[7] for being too icky. The "Peaceful Pill Handbook" is refused classification not because it advocates euthanasia, but because it advocates circumventing customs regulations. Clearly disregarding import restrictions is considered by legislators to be a source of societal outrage.

[6] The committee may be more familiar with this proposal being described as "filtering" – this is erroneous as filtering is considered to be something one does to one's own Internet connection, censorship is that done by a third party.

[7] Upon considering this submission, the committee should confirm the status of these films. Successive fights between attorneys general and the classification board see these regularly unbanned, rebanned, and then unbanned again. Meanwhile the Australian public interested in watching them simply buy them online.

The reality is that there is no "illegal content" on the Internet. None. Zip. Content cannot be illegal because criminal law does not provide for the criminalization of a *thing*. There is evidence online that warrants police investigation of crime, and there is *improper* material, but no evidence (despite a truly inspirational effort by 20 years of Australian regulatory history to muddy the waters) to suggest that the impropriety of improper material is something that Australians care an awful lot about.

We are certainly not in enough of a lather that we need "pseudo illegal" material to exist under the name RC, or we certainly resent the implication that we are irresponsible or immoral in not being grossed enough that a "super gross" category needs to exist for which we have increased regulation and censorship.

We may harrumph if they see something on TV not to our liking (but usually simply change channels), we may seek opinions of friends or movie reviewers before we go to the cinema, we may read the iTunes store's review of a movie we rent, or Zune HD's synopsis of a movie we buy for on-demand delivery to our TVs, but generally we have no need for or interest in, the opinion of a board of government chosen bureaucrats on this matter. We can look after ourselves, and those around us, and where we can't we expect the police to intervene.

The committee should propose that police and law enforcement agencies be required to provide details of what they require to ensure that content online which is evidence of the commission of a crime, including that which depicts child sexual abuse, be investigated. The committee should stress that successful investigation of evidence of crime online would require resourcing sufficient to enable international cooperation in a similar manner as is currently undertaken to investigate terrorism. The committee should report that the category of "refused classification" is an amorphous and uniquely Australian anomaly which serves no useful purpose but to inflict the values of a minority of Australians (the classification board, legislators and various attorneys general), onto the rest of Australia. Its continued existence, and its proposed expansion into a censorship regime, should be flagged for review by the committee with an ultimate aim of their abolition and a sensible classification system which more closely matches other contemporary democracies.

The committee should disregard submissions that insist, and advise against further committee conventions proposed to investigate, that illegal and inappropriate content online is materially different to the regulation of illicit drugs.

INAPPROPRIATE SOCIAL AND HEALTH BEHAVIOURS IN AN ONLINE ENVIRONMENT

TECHNOLOGY ADDICTION

There is no such thing as technology addiction. Thankfully on this matter (perhaps alone), the committee need not consider my carefully written submission which I provide from a decade of professional experience in technology and my proven record on technology policy. Matters of addiction are determined with authority by the DSM IV, the diagnostic and statistical manual of mental disorders, and are largely restricted to substances. Compulsive behaviours are sometimes referred to offhand as addictions but are more accurately termed simply as compulsive behaviours.

A child with an autism spectrum disorder can be observed to obsessively arrange toys within reach by size, shape, or some other metric. An adult with obsessive compulsive disorder may be similarly inclined (or feel compelled) to arrange items in colour or size grouping. To my knowledge, no joint select committee has ever been requested to look at the problem of people arranging things into groups.

The use of computers, the Internet or technology by an individual to an extent which is sufficiently more concentrated or prolific than average, is not a problem. There are many problems in society that may cause an individual to compulsively reach out to others using online channels, ignore pressing life problems by immersing themselves in an online game or other online behaviour. These are not problems with online behaviour; they are symptoms of social problems that people have had forever.

The committee should report that technology addiction is an inappropriate term for a newer manifestation of compulsive behaviour, and recommend that healthcare and social professionals be appropriately resourced to consider this manifestation together with the others with which they are familiar.

ONLINE PROMOTION OF ANOREXIA

Online promotion of anorexia is as prolific as online promotion of any other fringe belief and wholly as ineffectual on the numbers of people who actually come to hold harmful fringe beliefs.

The committee should report that consideration of the promotion of fringe beliefs is not an appropriate application of its time. The committee should not spend its resources considering promotion of anorexia to be a real problem online, but refer the matter of anorexia in general to the Department of Health and Ageing as a medically significant condition, the matter of education in the importance of healthy diet in young people to the Department of Education, Employment and Workplace Relations, and the issue of self esteem in youth as an aggravating factor in eating disorders to the Youth Bureau of the Department of Families, Housing, Community Services and Indigenous Affairs.

Drug Usage, Underage Drinking and Smoking

I make no submission on the effects of social behaviours online with regards to illicit drug usage, underage drinking and smoking. The very concept of depictions of these activities as an ***online*** issue that the committee ought to consider for the social welfare of Australians is an absurdity which plumbs new depths and does not deserve being addressed.

Identity Theft and Breaches of Privacy

These two items are separate bullet points in the committee's terms of reference but I choose to address them together.

While the prevalence of identity theft that is facilitated by the Internet is difficult to determine, it can be reasonably assumed that the globalisation created by the Internet means that Australians are providing personal information about themselves more than ever before, and doing so over greater distances than ever before.

There are two concerns that spring from this; confident details of an individual can be known by others leading to embarrassment and distress (and potentially to becoming the victim of a crime perpetrated by someone who could not acquire those details legitimately) or another individual using those details to identify themselves as the person to whom the details belong.

There are two circumstances where private information becomes known against an individual's wishes, regardless of what they are then used for. The first is when a repository of personally identifiable information is leaked or accessed in an unauthorised manner, and the second is when the individual is tricked into divulging them. The latter is referred to as "phishing".

Safeguards for private information storage are relatively straightforward from a technology perspective, and the ramifications of breeches well understood. It is an unfortunate side-effect of businesses that they would prefer to spend money on initiatives which enhance their profits than those which safeguard data repositories, and an unfortunate side effect of the public sector that regulatory hurdles and procurement processes interfere with technology best-practice in that sphere.

Phishing in Australia is enjoying a serendipitous combination of regulatory ignorance and popular gullibility. Australians hand over their personally identifiable information at a rate at least comparable to the rest of the world and there appears to be no intention by the government to assist in arresting the rate at which it occurs. "Safer Internet Day", a day which fell on the deaf ears of Australians due to woeful underinvestment by the federal government, was celebrated by the Australian Communications and Media Authority who warned (in no more impactful a medium as a press release, one wonders why they bothered) that young people post too much or inappropriate information about themselves on line. Young people are acutely aware of their privacy and how to protect it. They may have a different threshold for personal and confidential information than their parents had, and parents may be alarmed at the size of the audience to what is shared online, but adults hand over usernames, passwords and bank account details to fraudsters at a rate which *should* be significantly more alarming to regulators, but somehow isn't.

While the federal government ***could*** sensibly approach this issue of confident, digitally native kids online using technology to access community versus their parents who have "crossed the digital divide" but are still not fluent in the language spoken on this side of it, they don't.

Rather than fixing the key consumer privacy concerns facing Australia by using ACMA to produce a public-health style education campaign to adults explaining that no legitimate business will ask you for your password, the government takes a different approach. Senator Stephen Conroy from the Department of Broadband, Communications and the Digital Economy launched a breathtaking attack in Senate Estimates on organisations such as Google and Facebook, characterising them as prolific collectors and consumers of personal information, aggressively adverse to regulation and essentially nothing short of corporate criminals. Australians are not frightened of Google, and they are not frightened of Facebook. While social media sites trade sentiment and personally identifiable information for access to an online community, the participants in them are generally in control of their personal information and generally know fully what they are doing.

No Australians have had their bank accounts emptied by Facebook. Google has not impersonated any Australians at Centrelink.

The committee should recommend that hyperventilating about the privacy risks of online interaction be the sole domain of tabloid media. The committee should recommend that the ACMA take on an advisory and educative role in ensuring that fraud which relies on the ignorance of Australian users of the Internet be mitigated. The committee should recommend that public sector procurement processes and regulatory requirements for technology solutions that safeguard personal information against intrusion be streamlined. The committee should further recommend that private sector breeches be subject to severe penalties.

AUSTRALIAN AND INTERNATIONAL RESPONSES TO CURRENT CYBER-SAFETY THREATS (EDUCATION, FILTERING, REGULATION, ENFORCEMENT) THEIR EFFECTIVENESS AND COSTS TO STAKEHOLDERS, INCLUDING BUSINESS;

There are no international responses to current cyber-safety threats, because as previously mentioned we made up the term cyber-safety in Australia. Concerns about online regulation in democracies comparable to Australia are currently focused on either verifiably true and valid concerns about consumer interests, or issues such as the over-centralisation of infrastructure which may be a weak point to terrorist attacks, or concerns that Internet Service Providers may receive financial inducement to offer higher quality access to a particular resource at the expense of a competitor (referred to as "net neutrality").

OnGuard Online[8] – the US federal government resource which is as close to a "cyber safety" resource as can be applicably found, is an example which shows the United States' approach to consumer concerns. It currently focuses on phishing, spyware (software which is installed without an Internet users' consent, another are which the **committee should recommend the ACMA take on an educative role to combat**) and approaches any concerns with children using education for parents on how to engage with their children about their online experience.

The concept of mandatory filtering is utterly foreign in comparable democracies to Australia, and not possible in the United States due to the first amendment to their constitution. **The committee is unable to conclude that government control of content that Australians are able to access in the form of filtering is a best practice approach to Internet regulation, based on the experiences of other nations similar to Australia**. Countries where freedom of speech is severely restricted have mandatory filtering, countries in which the Internet industry felt that an inconvenient and pointless action was needed on a voluntary basis to pre-empt a breathtaking disaster in the form of a mandatory regulatory measure, have that[9].

Regulation of Internet content is something of a non-issue in other western-style democracies, they simply aren't as terrified of the Internet as we appear to be. Regulatory efforts around the Internet are focussed on its ability to ensure prosperity for business, open government and a connected population.

[8] http://www.onguardonline.gov

[9] The UK's voluntary filtering system is along these lines, the IWF was formed as "the devil you know" and has been responsible for a history of technical problems with the Internet there

OPPORTUNITIES FOR COOPERATION ACROSS AUSTRALIAN STAKEHOLDERS AND WITH INTERNATIONAL STAKEHOLDERS IN DEALING WITH CYBER-SAFETY ISSUES;

Within Australia regulatory bodies will be inundated with opportunities to cooperate with (or foster cooperation between) Australian businesses and non-government organisations on cyber-safety. Because this term is as unique to Australia as the fear our regulators hold about the Internet is, there is significant earning potential for security companies and censorware vendors who normally have to incite bespoke fear in regulators to conduct business with them. Not only are the types of preconceptions that security companies, academic grandstanders and handwringing child innocence advocates need to survive already present here, the government seeks to further develop an environment and framework of cooperation between them all. Fortunately they are largely non-damaging to Australia's approach to our online world, examples including the DBCDE "Consultative Working Group" not really breaking anything and the Youth Advisory Group on Cybersafety seemingly being ineffective as well. Private enterprise initiatives like Netclean Whitebox have excited government trials of censorship and made significant profits off it, but we are yet to see actual damage to the rights of Australians.

The committee should recommend that there is no need to foster further cooperation between the government and organisations, or within organisations, to ensure that fear-based instead of evidence-based policies are successfully mooted. The market ensures that bad policy is profitable by providing businesses and interest groups who have an interest in selling bad solutions.

EXAMINING THE NEED TO ENSURE THAT THE OPPORTUNITIES PRESENTED BY, AND ECONOMIC BENEFITS OF, NEW TECHNOLOGIES ARE MAXIMISED;

The statistical reality is that while a free market unhindered by fear-based regulation will usually come up with profitable and beneficial innovations, Australia is over-regulated and drives remaining innovation that was immune to our smaller population and economy, offshore. The NBN may go some way towards fixing this, but not if access to it is fettered.

The committee should recommend that current regulatory measures for the global digital economy, for which there is no international analogy, be considered for repeal.

WAYS TO SUPPORT SCHOOLS TO CHANGE THEIR CULTURE TO REDUCE THE INCIDENCE AND HARMFUL EFFECTS OF CYBER-BULLYING INCLUDING BY:

INCREASING AWARENESS OF CYBER-SAFETY GOOD PRACTICE;

Schools are aware of cyber-safety good practice because they are aware of safety practice. A necessary component of education and schooling is the safety of the children that attend there. While it is understandable that this evolves naturally with the advent of new technology, **it is not possible to identify a specific deficiency in aptitude for approaching bullying online versus offline that requires regulatory intervention or government interference.**

ENCOURAGING SCHOOLS TO WORK WITH THE BROADER SCHOOL COMMUNITY, ESPECIALLY PARENTS, TO DEVELOP CONSISTENT, WHOLE SCHOOL APPROACHES;

Schools are aware when and where to work within their communities to approach issues such as these, but government encouragement or being compelled by regulators is unwise. If there is any good to come from whole school approaches, or indeed whole of school-system approaches, it would be via **the committee advising that existing reporting structures for safety issues be expanded to include circumstances where misconduct is evident online**. That reporting should primarily, for criminal matters, be to the police.

AND ANALYSING BEST PRACTICE APPROACHES TO TRAINING AND PROFESSIONAL DEVELOPMENT PROGRAMS AND RESOURCES THAT ARE AVAILABLE TO ENABLE SCHOOL STAFF TO EFFECTIVELY RESPOND TO CYBER-BULLYING;

It has consistently been my submission that cyber-bullying is immaterially different from any other form of bullying other than the fact it is conducted using the Internet. Conduct on the Internet is faster and more effective in some ways than if conduct without an online environment. As a result, **the committee should recommend that professional development programs or training changes for school staff should be simply better resourced to offset the increased effectiveness of students who commit bullying offences using the Internet.**

analysing information on achieving and continuing world's best practice safeguards;

World's best practice is inapplicable in a country with a unique approach to these issues within a globally unique regulatory framework.

the merit of establishing an Online Ombudsman to investigate, advocate and act on cyber-safety issues

What would an online ombudsman regulate?

Because of Australia's economy and population, as well as our hostile regulatory framework, innovation in online technology and other online developments occur outside of Australia. As a result of this, popular websites such as Facebook, MySpace and Google are American companies subject to American jurisdictions.

In circumstances where globally acceptable benchmarks for bad conduct are breached, such as murder, theft, drug offences or other crime, extradition treaties are entered into for the purposes of mutually dealing with offenders. This spirit of cooperation between independent sovereign jurisdictions who have the same or similar values about human behaviour, is not repeatable when it comes to the Internet because of how different our approach is.

We have seen in the last months, Senator Stephen Conroy insist that the category of refused classification would be regulated by Google on their website YouTube. Google's response was to assert that they would do no such thing, that their own approach to their website is a result of corporate ethos and internationally accepted law, and that Australia's unique category of refused classification is entirely too broad for them to regulate on a website which has a global audience to which it is foreign and excessive.

What would an online ombudsman do in this circumstance? Insist louder that Australia's inconsistent and wholly inappropriate approach to content regulation be accepted by companies which are homed outside of Australia and are focussed on the whole world?

In circumstances where law has genuinely been broken, the police are able to cooperate internationally with their counterparts overseas (our AFP are well regarded internationally on these issues). What would an online ombudsman bring to the situation? Hearty congratulations to the AFP for doing their job of keeping us safe?

An online ombudsman would be wholly ineffectual, or be nothing more than a figurehead. **The committee should recommend that an online ombudsman not be established and that the concept has no merit.**

Conclusion

Australia has a uniquely broken approach to the digital economy, as evidenced by a committee convened to respond to it as an emergent threat, while other nations continue to find innovative ways of the Internet enabling prosperity, success and community.

The committee represents a unique opportunity to fix this, or alternatively may provide another "top coat" of regulatory pain on Australia and ensure that it may take decades for us to realise the same benefits from technology as the rest of the world.

I implore the committee to choose the former option, making a stand for the Australian community against the status quo of creeping regulation. I advise the committee that I would be delighted at any opportunity to give evidence to the committee, or clarify any points I have made in my submission.