SUBMISSION No. 15

Submission to the Joint Select Committee on Cyber Safety

Mark Newton

Submission to the Joint Select Committee on Cyber-Safety

Summary

Thank you for the opportunity to address the Joint Select Committee on Cyber-Safety.

I welcome the deliberations of the committee as an opportunity to provide the Australian Parliament with a realistic appraisal of the current state of the art of the Internet in Australia.

The Internet is a generational social phenomenon, with different implications for different groups of people. Like other communications technologies that came before it, such as the telephone, telegraph and the postal service, its prominence has heralded significant changes to the way our societies work.

We are currently in a state of flux:

On one hand we have a generation of people who have never known a time without ubiquitous Internet access, who have integrated it fully into their lives, using it fluidly and naturally, barely considering whether it's even possible to perform certain tasks without it.

On the other hand we have a generation of people brought up in the legacy of previous communications systems, who often don't understand the technology or the new social environments it is enabling.

Between the two extremes we have an amorphous mix of people with both attributes, who, in relation to the internet, are either fluent or foreign depending on the situation before them.

Overlaid on top of the whole mess is a media environment which seems purpose-designed to produce befuddlement for the uninitiated. Companies who are selling relatively straightforward products and services seek to differentiate themselves from competitors by using jargon and obfuscation to make them seem unique. Analogies which could help digital foreigners to find fluency are covered up: If you need to ask a question you're unlikely to be presented with an understandable answer, so the people who are most comfortable online are the people who never need to ask because they already know what's going on[1].

The generational effects produced by this state of affairs are not dissimilar to the effects encountered during other social upheavals. Whether we're looking at the introduction of the printing press, the popularization of the gramophone, the emergence of rock 'n' roll music, or the invention of the bikini, the same chronology is observed:

* A new phenomenon arrives, and is immediately embraced and understood by the young and/or progressive,

[1] Is the internet France?

* Those who don't embrace it or understand it treat it with suspicion, and imagine that it'll cause some arbitrary harm to society[2],

* After a couple of decades one notes that an entire generation has been born and raised in the presence of the phenomenon without ill effect, while an ever-shrinking group of suspicious minds continue to demonize it; and

* Eventually the suspicious minds either adopt the phenomenon themselves or die of old age, at which point the phenomenon becomes an entirely uncontroversial part of our social fabric. People write books about the panicky primitives of yore, drawing allusions between them and the mythical lawmakers who insisted that cars must be preceded on the roads by flagmen and limited to the speed of a horse.

The emergence of the internet is currently near the end of that evolution.

It arrived on Australian shores during the late 1980's. Since then, a whole generation has been brought up as natural internet users, and you can now walk into virtually any workplace and find a large coterie of Australians who simply can't remember a time before their home had Internet access. If the internet was actually dangerous, this entire generation of Australians would have been harmed by now, and our prisons and psychiatric hospitals would be filling up with internet victims[3].

Meanwhile, as those "digital natives" live happy and productive lives, those who have not adopted the internet to the same extent find it baffling, and ignorance breeds fear. The imagination runs wild. Scares are made-up from whole cloth. Movie plots seem real, because the observer lacks the in-depth knowledge required to separate fantasy from reality. Objectivity is lost, and the Internet seems like a frightening place.

With fear comes a desire to control, which pulls in the regulators -- and here we are today, with a confused and uncomprehending Government creating a Joint Select Committee to investigate the safety risks of something that virtually every schoolchild accommodates into their lives before they're old enough to read.

It's now 2010. The internet has been part of Australia's life for over two decades, and only now, after an entire online generation has been raised to adulthood and families of their own without online scars, we have an Australian Government which thinks "cyber-safety" is a problem[4].

To use a common online abbreviation: WTF?

It is difficult to comprehend the magnitude of the disconnect between the fear-based reaction of the Commonwealth and the enthusiastic uptake of the Internet by virtually everyone else in Australia. Australia has approximately 6 million homes connected to the Internet, we are among the most voracious early-adopters of new internet-based technologies, and internet connectivity is important enough to the electorate to turn the National Broadband Network (NBN) into a major political issue.

Yet anyone who listens to the Federal Government could be forgiven for thinking that there's some kind of uprising from the Australian people demanding protection from their fears, and that uptake is being inhibited because the online world isn't

---

[2] A variant of the Dunning-Kruger Effect, a cognitive bias in which "people reach erroneous conclusions and make unfortunate choices but their incompetence robs them of the metacognitive ability to realize it." http://en.wikipedia.org/wiki/Dunning–Kruger_effect

[3] It should be self-evident that they aren't, which should put perceived internet dangers into perspective: It either harbors dangers which Australians of all ages accommodate and manage with ease, or it isn't dangerous at all. There is no third alternative.

[4] A google search for the term "cyber safety" on 22 June 2010 reveals 1,420,000 results. One must advance to page 10 of the results to find a non-Australian use of the term. The moral-panic about "cyber-safety" is evidently a uniquely Australian obsession, with almost all of those first 100 search matches originating from Australian Government programs.

under sufficient Government control. Our major political parties have distinguished themselves as among the very last cultural institutions within this nation to "get" the internet.

This disconnect is corrosive to the credibility of the Government. When the electorate is populated by a vast number of people who *know* that the internet isn't harmful, politicians who hype online safety fears carry all the gravitas and authority of a 1950's parent telling her child that gyrating his hips to Elvis Presley songs will lead to loose morals.

To be taken seriously, one must say things that are true. Over the past several years, the Australian Government has established a track record and global reputation for being almost totally disinterested in truth as it pertains to online safety, pushing a grab-bag of poorly-targeted policies which don't stand the slightest chance of having any kind of worthwhile outcome[5]. This committee will be able to judge its success by the degree to which it is able to provide objective, verifiable evidence to influence the Government's so-called "evidence-based" policies.

The Online Environment in which Australian Children Currently Engage

Australian children access the online environment from virtually anywhere, at virtually any time, from virtually any device, using virtually any communications technology.

The technology itself is almost invisible, in the same way that the network of cables, satellites and telephone exchanges are effectively invisible when you make a phone call. Technology is merely a means to an end, and there's no requirement or desire from most people to understand how it works[6].

The technology acts as a substrate to support networks of conversations. A child might start a conversation with a group of friends in the schoolyard; then they might continue it by SMS on the bus on the way home; perhaps they'll use the telephone to continue it before dinner; then later, while they're doing homework, they'll progress it further by means of a Facebook chat window alongside their word processor and web browser.

Different technologies support different types of communication with different subsets of participants. A telephone call is one-to-one (or, at most, a 3-way call). A blog post is one-to-many. A comment thread on a Facebook post is many-to-many. Some communication modes support rich content such as video, audio, hyperlinks or still images; some are limited to text.

What will appear to an outsider as a distinct series of communication modes with distinct sets of participants, may actually be a single arc of social interaction which begins in a given time and place and extends for hours or days across a variety of different technologies.

Understanding the conversational nature of the interactions, and the fact that they're not affixed to any particular time and place, is key to understanding why childrens' use of media occasionally doesn't match adults' expectations (and why adult-imposed strategies for "managing" or "controlling" online behavior rarely have any appreciable effect). Adults don't use communication technology in the same way as children: When an adult finishes a telephone call, that's effectively the end of the conversation, few adults would consider following it up moments later with a blog post or an SMS.

---

[5] Latest examples: The House of Representatives' "Cyber-Security" committee, who inexplicably seems to seriously believe that Australians will use Anti-Virus software if Anti-Virus software is made mandatory; And ACMA's $100,000 "Cyber-Safety" red button, which, when pressed, instantly wraps a vulnerable child in a protective shroud of cotton-wool spun from Peter Garrett's spare stock of pink batts. Or something. God only knows what's actually supposed to happen when it's pressed.

[6] This observation distinguishes digital natives from digital foreigners. While those who have used the network for their entire lives show very little interest in its underlying implementation details, older generations use their unfamiliarity with the technology as an excuse to maintain their ignorance. One never hears a child walking away from a computer saying, "It's technical, I don't understand it." They don't perceive that it's technical, and don't care whether they understand it, they just get on with the job of using it.

The focus on "key physical points of access" imposed by this committee's terms of reference presupposes that children consider that various physical points of access are important. They aren't. Different points of access will have different capabilities and limitations, and will support different modes of communication; But if a child wants to say something and the access available where they are doesn't support it, they'll either find another way to say it or they'll wait until they're at a different physical point of access with different capabilities.

Similarly, the terms of reference's emphasis on "stakeholders controlling or able to influence that engagement," assumes that governments, parents, teachers, traders, internet service providers and content service providers are in a position to affect the child's conversational activities.

They aren't. Not even a little bit.

Throughout history, children have been able to create forums for conversational privacy (schoolyard discussions, exchanging notes at the back of the class, chatting while in transit to and from school, etc). The subject matter they discuss very often covers territory which authority figures would not condone; But the children don't care, and discuss it anyway. That's part of growing up.

Children are every bit as capable of creating space for conversational privacy online as they are offline. Furthermore, the skillfulness with which they manipulate the online world exceeds the ability of "offline" authority figures.

Every schoolteacher can report that the school's internet filter is ineffective at preventing kids from downloading whatever they want: they simply bypass it when it's inconvenient. Similarly, every parent can report that restricting a child's use of the telephone makes practically no difference to the amount of time they spend chatting to their friends: they use non-telephone technologies for chatting instead[7], and if the parent decides to use a home filter to prevent online chatting they bypass that one too.

The key message for this committee arising from this discussion is that **children don't use online technologies *as technologies*, they use them as enablers for social and cultural interaction.** There is no firm boundary between online and offline social interactions, and a child can just as readily hold a conversation with someone face to face in the same room or across the world via Instant Messaging systems.

Consequently, **attempts to control or influence children by technological means are bound to fail.** The technology is simply a means to an end, and if you use technical measures to inhibit it people will simply use different means to obtain the same end. The end effect will be to inhibit the technology without affecting human behavior[8].

One of the key failings of the Australian Government is to pretend that an offline occurrence magically becomes different, special and magical if you prefix its name with "cyber."

Thus the Government has wasted vast quantities of time focusing on "cyber-crime" when the real focus should be "crime."

Similarly, the Department of Broadband, Communications and the Digital Economy (DBCDE) is tilting at a trillion online windmills with its various chaotic "cyber-security" strategies, when the real focus should be "security" (which automatically moves the whole problem out of the realm of DBCDE and into the Attorney General's Department where it belongs).

The predilection of the Australian Government to pretend that the prefix "cyber" changes anything has been described by EFA Chairman Geordie Guy as, "Banning Murder on Thursdays."[9] Murder is already illegal, so passing a new law to make it

---

[7] http://www.reuters.com/article/idUSTRE63J4EX20100420 "Third of US teens with phones text 100 times a day", *Reuters, 20 April 2010.* A teenager who approximates 3000 text messages per month is *clearly* using the technology as a conversational medium.

[8] If non-Australian jurisdictions don't similarly inhibit their technology then the internet in Australia will be inferior to the internet everywhere else in the world, as the natural cost of imposing needless arbitrary technological limitations.

[9] http://www.geordieguy.com/?p=240

illegal on Thursdays is senseless. Similarly "stalking" is already illegal, it makes no sense to convene parliamentary committees to see if it can be made *even more illegal* if it's cyber-stalking.

This committee is looking at "cyber-safety." I put it to the committee's members that the real issue is "safety." Child abuse is child abuse; bullying is bullying; stalking is stalking; harassment is harassment. Whether they happen online or offline is totally immaterial to the victim and irrelevant to the perpetrator. The Government's response should and must be indifferent to the medium through which the crime is committed.

Although it is outside the terms of reference, I feel it's important to cover one more aspect of this issue, namely the locations where children *don't* conduct their online engagements.

Approximately two thirds of Australian households contain no school-age children. **Measures intended to control or influence online engagement by children which impact the requirements of adults who live in child-free households are, by their very nature, poorly targeted.** Our society in general, and our government in particular, ought not waste its limited resources on "child protection" measures which spill-over into affecting adults: Every dollar spent on imposing an unwelcome child protection measure on an adult is a dollar which hasn't funded a child protection measure for a child.

The nature, prevalence, implications of and level of risk associated with cyber-safety threats

It's disappointing that the Australian Government stands almost unique in the world in seeing online technologies as "risks" and "threats" rather than "opportunities" and "strengths." This goes back to the disconnect I described in my introduction, which hints at a society trying to rip ahead towards the future with gusto, held back by a timid, quivering, fearful Government who doesn't want to advance until the risks are all mapped-out and understood[10].

These "threats" also need to be kept in context with regard to their scope. For instance, this Government seems unnaturally preoccupied with "online promotion of anorexia," even though almost nobody in Australia is ever likely to see any online promotion of anorexia, and even though almost all of those who do will not, in turn, become anorexic[11]. That the Government spends so much energy on such a tiny "threat" strongly suggests that our public policy is dominated by whomever has the most overactive imagination and least-well-developed sense of proportion[12]. Those people ought to be ridiculed for our own protection, not put in charge of lawmaking.

The other factor which is germane to this subject is the seeming lack of understanding that the Australian Government shows to the difference between "risk" and "danger."

Crossing the street is an inherently risky activity, carrying the chance of instant death or serious lifelong injury. Yet we don't consider that it's a dangerous activity, because the risk is managed.

I put it to this committee that Australians are generally very good at managing online risk, and that children show a level of sophistication in risk management which is often unappreciated by adults because it's so effective that it makes many risks invisible.

---

[10] As every child knows: One must always wear a jumper when mummy is cold.

[11] The fact that the Government appears to have missed the fact that the only people who are influenced by anorexia promotion sites *are people who are already anorexic* is another manifestation of the "cyber" phenomenon I described in the previous section. Anorexia does not magically become different just because it's on a web page. If the problem you're trying to solve is anorexia, then *devote resources to solving the anorexia,* don't waste time and effort focussing on communication technologies.

[12] The author strongly suspects that each committee member reading this can readily roll-off half a dozen names of people who fit that description.

Cyber Bullying

The fact that childrens' conversations are no longer limited to a particular time and place affects the nature of bullying.

In our parents' days, bullying was a relatively simple affair: A child would have a miserable time when they were in contact with the bully, and would suffer gossip while within the sphere of influence of the bully's friends (who could be considered sufficiently complicit to be bullies themselves).

A playground, a sporting fixture, or similar could be a terrible place for the bullied child. Most of us would know at least one family member who (for example) didn't want to go to school due to bullying. Home was a safe-haven, school wasn't, so the child would want to stay at home.

Bullying in the 21st century has changed little, except that now the toxic conversations which rob a child of their self esteem are enabled by the same technological substrate which enables every other mode of conversation, which means bullying is no longer limited to a particular time and place. The always-on nature of modern communication means that the child can be bullied 24x7 without regard to where they are or what they're doing. There is no safe-haven, no let-up, no relief, no way to escape. The child can't read their email, contact their social networks, or read the text messages on their mobile phone without letting the bullies into their lives.

The skillfulness with which children are able to construct conversational privacy makes bullying easier too: The bullies are able to hide their activities from authority figures; And the victim, whose self-esteem is likely to be tied to whether they'll be forever labeled a "sissy" by involving a parent or teacher, or exposed as a victim before their non-bullying friends, will work hard to keep their victimhood as private as possible.

The end result can be that parents and teachers will have no idea that some of the children in front of them may very well be bullying another child before their very eyes; and observers of the victim will note that he or she will be progressively more withdrawn, sullen and unhappy, but insensitive to the reasons why.

Government responses to date have ranged from ineffective to destructive.

DBCDE's "Cyber-Safety" red button edges towards the hilarious side of ineffective: No bullied child is going to contemplate pressing a panic button to call in the authorities, the whole idea is so absurd as to be beneath contempt, one of those ridiculous ideas that's difficult to mock because it's already been used to parody something else and its humor value is all wrung out[13].

On the destructive side we have the misguided advice of Mr. Kevin Rudd, who recommended that parents contact each other about bullying[14], leading to psychologist and bullying researcher Dr. Helen McGrath to warn that parents of bullied children who contact parents of bullies will find that, "... things often become hostile and can get out of hand and make the situation even worse." Queensland Secondary Principals Association president Norm Fuller saw fit to respond to Mr. Rudd's remarks with a warning about violent vigilante behavior.

This committee should be aware that bullying is a reasonably well understood issue, an area of active psychological research with recognized experts in the field giving known-good advice. The problem scope is known, the feasible solutions are pretty well understood too. It isn't a technology problem, and it cannot be solved through technology policy. Treating it as a "cyber-problem" is profoundly misguided.

Cyber Stalking

Many of the comments I've made about bullying also apply to stalking.

---

[13] http://giftsaustralia.com.au/?action=view&id=1094011

[14] "Experts slam Kevin Rudd's Advice on Bullying", *Courier Mail, 4 March 2010* http://www.couriermail.com.au/news/experts-slam-kevin-rudds-advice-on-bullying/story-e6freon6-1225837149786

The aim of a stalker is to undermine the victim's sense of personal security. A stalker will use any means available to carry out their task: Physical presence, telephone calls, letters, text messages: Anything that makes the victim think about the stalker.

Stalking appears superficially similar to bullying, and, like bullying, online technologies can make it pervasive for the victim. The online world can also assist a stalker by providing access to any parts of the victim's life which have been published online with inadequate privacy: Blogs, networks of acquaintances stored by social networking sites, photographs on personal websites. Any personal information the victim has published during the entirety of their pre-stalked life can aid the stalker.

Unlike in the case of bullying, a stalker's victim is unlikely to want to keep the matter private. Once a stalker is reported to law enforcement authorities, their electronic footprints make them relatively easy to identify.

The *risk* of online stalking is real, but the *danger* of online stalking is so low that the term "cyber-stalking," is used ironically by internet users to refer generically[15] to the act of acquiring public information about someone for virtually any purpose. Yes, there are a very small number of real victims who have been stalked by people using online technologies, but the technologies were simply a means to an end. Australia didn't commission Parliamentary enquiries to investigate the telephone network when stalkers first started making phone calls, or the postal service when stalkers discovered the psychological impact of sending threatening letters by mail. **Is any realistic stalking *danger* presented by the Internet that isn't also presented by literally any other method of making contact with another human being?** Treating the crime of stalking as somehow special just because it makes use of the online environment is simply another example of "banning murder on Thursdays."

Sexual Grooming

Nowhere has the Parliament's abdication of objectivity in relation to online threats been more obvious than in the field of child sexual abuse.

We live in a country in which *almost no* citizens are child sexual abusers. According to research carried out by the Australian Institute of Criminology[16], Queensland official statistics indicate that the rate of sexual offenses reported to police was approximately 190 per 100,000 population in 2001 (less than one fifth of one per-cent), and that, "There is no clear evidence ... that the incidence of child sexual abuse itself is increasing," observing that reporting rates are climbing as society reaches "... widespread agreement that child sexual abuse is a major social problem."

If one counts the number of hours this Government has spent obsessing over child sexual abuse in the online environment, however, you could be forgiven for believing that there was a growing, widespread, national child-rape emergency fueled and enabled by the internet.

There simply isn't. It's another moral-panic[17] in the long string of moral-panics that a long series of Australian Governments of all stripes seem to be addicted to.

It is objectively true that the population of children who are sexually groomed is so tiny that it's lost in the statistical noise, and the population of abusers who groom them is even smaller.

---

[15] Example: "Facebook stalking becomes even easier," *Asher Moses, Sydney Morning Herald, 10 March 2010* http://www.smh.com.au/digital-life/digital-life-news/facebook-stalking-becomes-even-easier-20100310-pyb8.html Note that the detail of the actual article refers to a facility which enables Facebook users to choose to display their location on a map; *Looking at the map* is described as "stalking."

[16] http://www.aic.gov.au/documents/1/D/7/%7B1D7F5F5E-2B6A-44CA-B2CB-9B330AE888A8%7Dti193.pdf "Child Sexual Abuse: Offender Characteristics and Modus Operandi", *Stephen W. Smallbone and Richard K. Wortley*

[17] http://en.wikipedia.org/wiki/Moral_panic

A curio with respect to the issue of sexual grooming is that many of the children affected welcome the approaches, appreciate the attention, and keep the conversations secret from their parents. Awareness programs in schools aimed at children, and other forums aimed at parents can be effective in uncovering it in the unlikely event that it ever happens.

The Australian Federal Police (AFP) retains world-recognized expertise in tackling criminals who groom children, online and off. Their Online Child Sexual Exploitation Taskforce (OCSET) is capable and effective, and deserves significant expansion.

The difference between the "cyber-safety" rhetoric emanating from the current Government and their actual concrete policy is laid bare by observing how they've treated OCSET.

The previous Government allocated $51.8 million in the 2007 budget to enable OCSET over the 2009-10 timeframe to fund "additional 90 staff" members[18]. The Rudd Government cut the allocation to $49 million (a $2.8 million reduction), delayed the funding until 2010-11, and changed the headcount to "91 additional AFP members dedicated to online child protection"[19] (implying that they'd be expected to take a pay cut relative to what the Howard Government had allocated).

Sexual grooming represents a risk, but not a significant danger. **An adequate response to sexual grooming would be to increase the resources available to the AFP so that they are better able to investigate and arrest child abusers.** Implementation of policies which treat online child abuse as a special case of all child abuse are most likely to succeed: Child abusers are criminals regardless of whether they use the online environment as one of the vectors for their abuse. Policies which pretend that proximity to the internet makes any difference to the actions of the abuser or the impact on the victim cannot survive objective scrutiny.

Exposure to illegal and inappropriate content

The current Government has conflated the terms "illegal content" and "inappropriate content" by pursuing its profoundly unpopular ISP censorship plan.

The Minister for Broadband, Communications and the Digital Economy has, at various stages in the continual evolution of the policy, portrayed various types of *legal but controversial* content as if they were illegal.

Illegal content is very clearly defined in Australia: The only way content can become illegal is if it is the subject of a judicial finding pursuant to a State or Commonwealth law[20]. Such content is (and always has been) so vanishingly rare that the vast majority of Australians will live their entire lives without seeing any of it, and is adequately dealt with by the AFP.

Material which has not been the subject of such a finding can, at most, be, "suspected illegal," or, "allegedly illegal."

The current Government has created the manifestly false impression that material can become illegal by means of a decision by the Commonwealth Classification Board to rate it as "Refused Classification" (RC).

RC content is not, and never has been, "illegal." It is lawful for Australian citizens to possess, own, read/view, give away and purchase RC content in all forms, except in Western Australia (which has a State law which criminalizes possession of RC content) and parts of Western Australia and the Northern Territory associated with the Aboriginal Intervention (where possession of content rated higher than MA 15+ is an offence). It is also legal to transmit RC content over a telecommunications network everywhere except Western Australia.

---

[18] The additional allocation was partly in response to allegations that OCSET was so starved for resources that it was referring its caseload to State police forces. See "No money available to chase internet pedophiles," *Luke McIlveen, Daily Telegraph, 18 June 2007.*

[19] http://libertus.net/censor/isp-blocking/au-govplan-p2.html#s_38 "Budget for Australian Federal Police's Online Child Sexual Exploitation Team," *Irene Graham, 2009.* Includes cites to 2007 and 2008 Budget Papers.

[20] For example: The Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004, which contains definitions for "child abuse material" and "child pornography material," and creates various offences pertaining to transmitting such material using a carriage service.

Under Australian law, the RC category is intended to create a restriction on commercial exploitation. RC content cannot be sold, exhibited in cinemas, or imported into Australia for commercial sale.

It is nevertheless lawful for Australian citizens to acquire RC content for their own enjoyment if they so choose, consistent with principle (A) of the Commonwealth Classification Code[21], which states, "Adults should be able to read, hear and see what they want."

An Australian is breaking no law by buying the internationally acclaimed RC film *Ken Park* from amazon.com[22]. An Australian is not committing an offence by viewing the RC film "70K Krew" on Youtube[23]. An Australian is not committing any crime by reading an RC account of a technique for making blackpowder[24]. Australians who peruse the written opinion of the Full Bench of the Federal Court containing the copy of the RC article *The Art of Shoplifting*[25] from LaTrobe University's student newspaper *Rabelais* will not, themselves, need to answer to the Full Bench of the Federal Court.

Furthermore, *there is no other jurisdiction on the entire planet who would even think of restricting access to any of that content.* The RC category is uniquely Australian, existing as a limbo-land between unambiguously legal and unambiguously illegal: "It's legal, but we really want you to pretend it isn't."[26]

The RC category is an expression of a community standard: When the Parliament of Australia wishes to tell Australian voters what it believes to be "unacceptable content," it amends the definition of RC to suit.

The entire Classification Board architecture operates in a similar vein: "Here is the set of content which we, Australian MPs, believe is suitable for 15 year olds. Here is the content which we, elected officials, believe is suitable for children."

The beliefs and wishes of the wider community are ignored at best, treated with contempt at worst[27]. There have barely ever been any broad community consultations into the compatibility between the Classification Guidelines and actual Australian community standards.

So let me tell you how classification works in Australia:

Australian parents of very young children don't care about classifications, because they're irrelevant. Parents of very young children will either supervise children during their consumption of content, or only make available items which are objectively intended for young children. Such a parent doesn't care that the film *Texas Chainsaw Massacre* is rated R18+, because there is no possibility of *Texas Chainsaw Massacre* appearing on the menu of available media choices the parent will present to the child. Similarly, the Classification Board's judgement that *The Wiggles* is rated G is also irrelevant, because the parent

---

[21] http://www.comlaw.gov.au/comlaw/Legislation/LegislativeInstrumentCompilation1.nsf/0/4044954899915EE76CA25741100165EFA?OpenDocument Guidelines for the Classification of Films and Computer Games

[22] [redacted]

[23] [redacted]

[24] [redacted]

[25] http://www.austlii.edu.au/au/cases/cth/federal_ct/1998/319.html

[26] http://www.itnews.com.au/News/163063,commentary-why-we-dont-need-a-filter.aspx "Commentary: Why we don't need a filter," *Mark Newton, iTNews, 17 December 2009.* Introduces Aunt Gladys from Cootamundra, who has never used the internet but has very strong opinions about it -- and for whom the RC category is tailor-made.

[27] For example: When the ABA surveyed the population and found that 82% of 2240 Australian adults should have the option of watching R-rated programs on pay TV, the Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies recommended banning R-rated programs on pay-TV, claiming that adults surveyed answered the way they did because they didn't understand what R-rated material was. http://www.aph.gov.au/library/pubs/bd/1997-98/98bd060.htm#Background

isn't an idiot, and has no need of any assistance from Commonwealth regulators to work out that *The Wiggles* is intended for children.

Parents of young adults take a somewhat different view: They arrive at the conclusion that there is no point in trying to control the content that their children consume, because their children will consume it whether they like it or not. It has always been so, ever since the first 15 year old stumbled across Mum's stash of porn in the bottom of her underwear drawer, or found Dad's dirty movies hidden in the back of the liquor cabinet. If parents have done their job correctly during the child's formative years, they'll know that the values they've instilled in their child will ensure that there is virtually no risk of harm arising from their consumption of "unapproved" content, regardless of the Classification Board's rating. The opinion of the Classification Board is, therefore, irrelevant to these parents.

Adults consuming content on their own behalf don't generally pay a lot of attention to what the Classification Board thinks either. If I want to view *Reservoir Dogs* or *Up!* I'll simply watch them. Australians rarely check ratings on content (except when we're actively seeking X18+ explicit content). We don't need the Classification Board's opinions pertaining to our own media consumption choices, because we're clever enough to work those things out for ourselves.

The Classification Board's useful role is therefore confined to providing advisory information to parents of children who are old enough to deserved reduced supervision, but not so old that they're listening to their peers instead of their parents. A span of perhaps three years, from age 9 or 10 through to approximately age 12.

In that context, any ratings other than PG and MA probably serve no useful purpose.

Of course, while all of that is going on, the Classification Board isn't the only game in town. It's only responsible for classifying books, periodicals, films in cinemas, DVDs and videocassettes, internet content and computer games.

There are other classification bodies available for content delivered in other forms:

* Free to air commercial television operates its own classification system under the Free TV Australia industry code,

* ABC and SBS each operate their own separate classification systems (the drafters of the *Broadcasting Services Act* literally forgot about noncommercial broadcasters, so they weren't originally covered by the same terms as the commercial broadcasters),

* Subscription television classifies its own content,

* Airlines classify special all-ages cuts of their films,

* Content available from internet sources is either classified by its country of origin or not classified at all,

* Users of content distribution systems such as *Apple iTunes* can choose the classification system they want to use by altering a configuration parameter.

So one can consider an item of content classified M. Is it the commercial TV "M"? The Classification Board's "M"? The airline "M"? The "M" used by the MPAA in the United States? They're all subtly different, how is a parent supposed to know?

We live in a world where content can come from anywhere, and almost none of it is examined by the Classification Board, and almost nobody in Australia could care less. No Australian who has ever illegally downloaded an American edit of a Hollywood blockbuster has ever said, "Oops, can't watch this, it's rated NC-17, I need to know what the Australian Classification Board thinks."

To media consumers in Australia, the opinions of the Parliament of Australia as expressed by the Classification Board are almost perfectly worthless[28].

Even if one pays attention to the Classification Board it sends confusing signals.

Consider the film *Salo: 120 Days of Sodom.* When it was originally released in 1976 it was immediately banned in Australia.

Then, according to our Classification Board, something incredible happened to Australian society in 1993, because we all became intellectually sturdy enough to view the film without turning into axe-murderers, allowing it to earn an R rating.

Five years later in 1998, a magic unicorn died somewhere, which was a shame because *it was that unicorn that was emitting rainbow-coloured mind-rays which were making Australians intellectually mature enough to view the film.* Upon the unicorn's death, we all became so feeble-minded that the Classification Board needed to ban *Salo* again for our protection, and the protection of our community standards.

In March 2010, the Classification Board decided that the film isn't brain-meltingly abhorrent after all, and perhaps we're mature enough to see it again, but only if we're good.

But our erstwhile Minister for Home Affairs, Brendan O'Connor, doesn't agree[29]: He clearly believes Australians are too fragile to withstand the assaults of the film, and he's asked the Classification Board to reassess it[30]. Australia's Parliament lacks so much objectivity that we are confronted with the spectacle of a politician who seriously believes that he'll earn votes by claiming we're all too stupid to watch a film without hurting ourselves, then launching himself into the breech to protect us from our own choices.

This state of affairs is, frankly, asinine. Although *Salo* isn't a particularly pleasant film, it has been available in virtually all parts of the world throughout the entire time in which it has been banned in Australia, with no ill effect whatsoever. It is absurd to suggest that French people, Italians, Britons, Americans, Canadians and Mexicans are perfectly capable of viewing such a film without causing the downfall of their respective societies, while Australians are so mollycoddled and brittle that the mere *availability by mail order* of such a film requires emergency Ministerial attention.

To the Australian Government: Stop panicking about media, please just grow up.

Our classification system is based on the nebulous concept of "community standards," loosely defined as, "the standards of the community comprised of MPs." Australia's multicultural and multigenerational society is comprised of lots of other communities, with lots of differing community standards.

There are communities of Christian fundamentalists online. There are also communities of people who see humor in "2 Girls 1 Cup."[31] Whose community standards ought to define the limits of acceptability?

When the Minister wins his reassessment and the Classification Board re-bans *Salo*, Australians will continue to do what they've been doing for years: They'll download the film with *BitTorrent*, burn it onto a DVD, and watch it in spite of the Classification Board's judgement. Enabled by the NBN, they'll be able to do it quicker than a visit to the DVD store at the local mall.

Our modern electronic media landscape has rendered the Classification Board obsolete.

---

[28] It's even worse for computer gamers: They receive the opinions of the Classification Board with rank hostility, and live under no pretensions whatsoever about whether the Classification Board is representative of "community standards."

[29] It's terrible when mummy and daddy fight in front of the children.

[30] http://www.ilsac.gov.au/www/ministers/oconnor.nsf/Page/MediaReleases_2010_SecondQuarter_16April2010-MinisterRequestsReviewofSaloClassifcation

[31] [redacted]

Our entire classification system needs urgent reform to update it for our modern communications technologies. In its present state almost nobody pays attention to it; Those who do pay attention to it are confused by its misleading inconsistency; Those who understand why it is inconsistent are contemptuous of its sheer idiocy.

A reformed classification system for the 21st century would have the following attributes:

* It would assume from first principles that the Government is completely incapable of controlling the distribution of legal content, and would therefore not undermine its own credibility by making the attempt,

* It would be media-independent, allowing the same consistent system to be applied to content regardless of the form of its transmission,

* It would not be compulsory: There is no value in applying a special Australian rating claiming that *Mad Max* is suitable for viewing by adults when it has already received ratings saying it's suitable for adults from the UK, Ireland, Italy, Argentina, Canada, France, New Zealand, Norway, South Korea, Spain, the USA, Germany and Finland. If other classification systems have already rated an item of content, Australian consumers should be permitted to be guided by them if they trust them more than the Australian system,

* Guidelines should be established for approval of rating systems operated by third-parties such as NGOs and foreign governments (for example: If people choose to trust Young Media Australia's ACCM ratings[32] then they should be entitled to do so). The presence of a rating from *any* approved rating system should satisfy Australian classification requirements. Australia is comprised of lots of communities, customized content ratings can be provided to all of them if they so desire.

* Ratings applied by the reformed system would be explicitly separated from any judgement as to legality or illegality.

* The "Refused Classification" rating would be abolished entirely, bringing Australia's system closer to compatibility with literally every other classification system in the world.

This committee should recommend that **Parliamentary consultations should be carried out to establish parameters for a reformed classification system for the 21st century carrying the attributes outlined above.**

Without taking that step, Australian parents will be forced to continue with the current systems, which are chaotic, contradictory, misleading and almost entirely irrelevant to contemporary community standards; And, for the foreseeable future, our Parliament will continue to impotently huff, puff and beat its chest about the way in which Australian children are *daring* to consume "inappropriate" content against the wishes of the Classification Board.

Inappropriate social and health behaviors in an online environment

While there are concerns about inappropriate social and health behaviors online, I cannot agree that the list of examples attached to this term of reference ought to be taken seriously.

"Technology addiction" is a made-up problem[33]. The Chinese seem to take it seriously, but we all know that they're just using the concept as an excuse to punish dissidents[34] under the cover of a purely invented psychological ailment.

The Government's unhealthy obsession with the online promotion of anorexia has been adequately covered elsewhere in this submission, and need not be reexamined here.

I find it unfathomable that anyone could suggest that drug use, drinking or smoking could possibly be a "cyber-safety threat." Are there people who imagine you can take a drink from a mobile phone, or smoke a cigarette on the internet? Or

---

[32] http://www.youngmedia.org.au/mediachildren/07_04_choose_films.htm

[33] Did Parliaments in the 1600's complain of "book addiction" following the popularization of the printing press when young people read more books than their illiterate parents considered healthy?

[34] http://www.timesonline.co.uk/tol/news/world/asia/article6739615.ece "Chinese teenager beaten to death in internet addiction clinic", *Jane Maccartney, The Times Online, 5 August 2009*

is the committee referring to the fact that the internet makes alcohol and tobacco advertisements from countries which don't share our advertising laws available to Australians? If so, my recommendation to the committee would be, "Get over it."

Inappropriate social and health problems need to be dealt with as social and health issues, not "cyber" issues. Our society's institutions have been accommodating these problems for years, with considerable success and expertise. Rather than reinvent the wheel by treating online versions of these issues as distinct problems, **the Committee should recommend that awareness of the online environment be built-in to existing social and health programs.**

For example: Anorexia is a problem which is already treated by a variety of State and Commonwealth programs. Educational materials could be added to existing information resources for carers, sufferers and treatment practitioners to ensure that any aspects of the sufferer's disorder pertaining to the online environment are adequately accommodated by their personalized treatment program.

Identity Theft

Identity theft isn't an artifact of the online environment so much as a side effect of the distributed nature of our modern societies.

Turn the clock back a century and identity theft was unheard of. Everyone knew their neighbors, had reasonably well-known reputations in their local area. They'd bought milk and bread on the way home from work at the same shop for 20 years. They knew their local bank manager and tellers, local police, business owners and so on.

In that environment, "stealing" someone's identity was difficult: Attempts to impersonate someone in their local area would fail because they were well known. Attempts to impersonate them outside of their local area were pointless because their identity only had value to the extent bestowed by its reputation.

As our communities have grown larger and more impersonal, those safeguards against impersonation have broken down.

We transact business with banks without ever visiting a branch and meeting a human face. We shop at chain stores with high staff turnover. Police rarely interact with the public in any meaningfully personalized way. We've never introduced ourselves to our neighbors, and have no reason to believe we won't have different neighbors next week.

The business world has accommodated those changes by bestowing reputational value on pieces of paper, entries in databases, and numbers stamped into plastic cards. While they have certain safeguards around those items of data, the protection is necessarily porous: a reputation is pointless if it isn't well known by those with whom you transact, so spreading those semi-private bits of identity relatively widely and freely becomes a necessary prerequisite for business.

And so we get to identity theft: If someone who isn't you can lay claim to your numbers and database records, they can adopt your reputation and pretend to be you.

This is another example of a non-technical occurrence assisted by the communications substrate provided by the online environment. And, like all the other examples, attempting to control it by regulating the communications substrate is profoundly misguided.

Identity theft is, at root, a con game. The con artist uses exactly the same techniques to steal your electronic identity as she'd use to impersonate you "in the flesh." It's a game of bravado, where they attempt to gather enough information about you to credibly pass themselves off as you to one individual or organization, then they use that forged relationship as a credential to leverage themselves into new individuals and organizations[35].

Australia's strong privacy protection laws place us in a good position to fight identity theft, and my observation is that we seem to be better at it than our American cousins.

---

[35] In the same way that one can forge a piece of paper which looks like birth certificate, and attempt to use it as a credential for the issuance of a passport.

For example: American identity theft is often enabled by their use of Social Security Numbers (SSNs). There are virtually no privacy protections on SSNs, and Americans must provide them for all sorts of reasons. Employers ask for them on job applications, police check them during pull-overs, utilities require them as a unique identifier for billing, hotels ask for them in lieu of a credit card if you're aiming to pay your bill in cash. Every American leaves a trail of SSN breadcrumbs through the entirety of their financial life.

The typical question a company will use to verify your identity is, "What's your date of birth and your SSN?" Birthdays are trivial to determine, and SSNs are so liberally spread across American commerce that it's almost impossible to avoid them, so the end result is that it's almost pathetically easy to accumulate enough credentials to enable you to pass yourself off as someone else.

The Australian Government's equivalent of the SSN is the Tax File Number (TFN). There are strict privacy regulations on the use of TFNs, with severe penalties for transgressions. It is very difficult for most people to establish someone else's TFN; and, once they know it, it's useless for identification purposes because Australian businesses and Government departments don't accept the TFN as a credential.

While we read articles in the American press warning about the prevalence of identity theft, we need to be mindful of the fact that *we're not them,* and our antipodean attitude towards privacy is part of an effective protection against impersonation.

To continue to minimize identity theft in Australia, **this Committee should recommend that the AFP survey known cases of identity theft to determine the vectors by which offenders were able to obtain the victim's private information. The Committee should further recommend that the Australian Privacy Commissioner use that data to consider whether future leaks of the same information might be prevented by strengthening our privacy protection laws.**

Identity theft is incompatible with strong privacy protection -- If fraudsters are prevented from obtaining secrets about their victims, they can't credibly impersonate them. Our privacy protections should be periodically reviewed to ensure that they aren't outpaced by changes in the way that contemporary businesses operate.

Australian and international responses to cyber-safety threats

It's difficult to make a strict comparison between Australia and the rest of the world on "cyber-safety" threats in 2010 because the Australian Government is virtually unique in believing that "cyber-safety" even exists as a concept.

The idea that the internet is a threatening place deserving of special governmental attention, fearful advisories to parents, and onerous restrictions on children appears to be a uniquely Australian perspective. Which is odd, because everyone in the world is using the same internet: Why does the Australian government view it as a threat where the rest of the world finds it comparatively mundane?

Our citizens certainly don't find it threatening. Australians have been utterly voracious in their adoption of online technologies: There are now more than 6 million internet subscribers in Australia[36], and more active mobile phone accounts than there are people. The Australian Communications and Media Authority (ACMA) has also produced extensive research over many years which all shows that Australian families veritably *love* the internet[37] [38].

---

[36] http://www.abs.gov.au/Ausstats/abs@.nsf/0/528E278D97686C2DCA25723600064DD7?opendocument ABS 2007 Year Book Australia, "Internet Activity."

[37] http://www.acma.gov.au/WEB/STANDARD/pc=PC_311655 "Australia in the Digital Economy: research report series", ACMA, 2009

[38] http://catalogue.nla.gov.au/Record/3509539 "KidsOnline@home: Internet use in Australian homes", *ACMA, 2005*, which reports that less than one third of households "use computer software to block websites," and of the parents who don't use filters, more than two thirds "Trust child, don't feel need to do this," or believe that, "Other safeguards are sufficient."

So why does the Government believe (as this one surely does) that Australians find the online environment "threatening," and desire or require to have it brought under the control of politicians?

Virtually our entire country is online, and we've brought up an entire generation of digital natives who are comfortable and familiar with computers. So why does the Government believe (as this one surely does) that the *number one* IT issue in the entire country is massive untapped demand for internet censorship by ISPs?

It just doesn't add up. The Australian Government clearly isn't serious about the online environment. Fear is triggered by ignorance, and nobody is more ignorant about the internet than the current Australian Government.

Our international peers got over this years ago. The USA dabbled with fear in the 1990's, passing the *Communications Decency Act* (CDA) during the Clinton administration to censor the internet. But appetite for that level of control was all but gone by 1998 when the US Supreme Court found the CDA unconstitutional. They've not made any serious effort to revisit the matter since.

The UK was similar: The Internet Watch Foundation (IWF) was formed in 1996 to operate an optional blocking service. While there have been occasional murmurs from the radical fringe to make it compulsory, 14 years of opportunities to do so have been passed up. In its most recent annual report[39], the IWF has suggested that the prevalence of illegal content on the web appears to be diminishing (from an already infinitesimal base), and that approximately two thirds of all illegal content appears to be published by ten organizations (strongly suggesting that coordinated police attention could clean the mess up once and for all -- But where is the appetite for that among the world's governments?).

In 2008 Google reported[40] that it had indexed one trillion webpages, and that the web was growing at the rate of approximately one billion URLs per day. Assuming that growth rate is linear, the size of the world wide web is rapidly approaching 2 trillion URLs, with no corresponding increase in the amount of child abuse content. Is it any wonder that our Communications Minister lacks credibility when he suggests that the Government seriously believes in the importance of spending $44.5m worth of taxpayers' money on an ISP censorship scheme to block a mere 355 URLs[41]?

Other countries don't have "responses to cyber-safety threats," because the concept of "cyber-safety threats" is almost unique to Australia. The rest of the free world just doesn't see the internet in those terms. Our international peers see the internet in terms of opportunity, economic growth, and societal betterment, not fear, threats and harmed children.

There is only one internet. Why is our Parliament's view of it so different from everyone else's?

Opportunities for cooperation across Australian stakeholders with international stakeholders in dealing with cyber-safety issues

Opportunities for international cooperation in dealing with cyber-safety issues are complicated by our policy of internet isolationism.

For example: We inexplicably maintain an insistence that Refused Classification content should be heavily regulated. *No other country in the world recognizes anything like our Refused Classification rating, so Australia's appeals for regulation consequently fall on deaf ears.*

The most recent example of this international disconnect concerns the falling-out between DBCDE and Google over the Labor Government's ISP censorship policy. The Minister has proposed that Google should censor Refused Classification

---

[39] http://www.iwf.org.uk/media/news.285.htm 2009 Annual Report, Internet Watch Foundation

[40] http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html "We knew the web was big..." *Google, 25 July 2008*

[41] http://www.aph.gov.au/senate/committee/priv_ctte/report_145/e02.htm Response by Mr. Geordie Guy, Board Member, Electronic Frontiers Australia Inc. on behalf of the board members of Electronic Frontiers Australia Inc., incorporated into Senate Hansard on 23 June 2010.

content. Google has, by all accounts, pointed out that it's a company based in the USA, where RC content isn't illegal, and it therefore simply will not cooperate with Australia.

That failure to engage is not Google's fault, it is the Australian Government's fault. Abolition of the RC category would change the conversation, to one where Australia said, "We believe illegal content should be heavily regulated," and Google would say, "Great, but we don't have any illegal content. We comply." End of argument.

Where content and conduct is objectively illegal, the AFP enjoys considerable cooperation from international law enforcement agencies whether the illegality occurs online or offline. Again, the "cyber" prefix is a distraction. Fraud is fraud, identity theft is identity theft, pedophilia is pedophilia, harassment is harassment. These offenses are simply illegal, and the use of the online environment to commit them makes very little difference to anything.

Examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised

The actions of the Australian Government can have a large impact on the availability of opportunities presented by new technologies, and their economic feasibility.

If the NBN is built, and services are able to be offered over it to Australian consumers at prices they are willing to pay, it will act as a "great leveler" by presenting opportunities to all Australians to integrate broadband internet access into their lives.

But the access provided by the NBN is of limited worth unless services and applications can be freely delivered over it.

The statistical reality is that most online service innovations will be developed outside of Australia, due to the fact that almost all internet users and almost all internet-based companies are located overseas.

If citizens of other countries can utilize newly developed technologies in ways that Australians cannot, then Australians will not reap the full benefits.

Undue restrictions on Australians also make other jurisdictions more attractive places to host innovation, driving R&D dollars offshore.

The Government can assist in the maximization of benefits arising from new technologies by ensuring that its treatment of those technologies is no more restrictive than the treatment the technologies receive in the other jurisdictions in which they are used.

The internet abhors bureaucracy. In many cases, the best thing the Government can do to maximize online opportunities is to stay out of the way.

Ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bulling

The issue is not "cyber-bullying," it's just bullying. Until the Government accepts that simple fact, nothing it does will have any impact at all on the phenomenon.

Bullies have never been limited to the schoolyard. Children can be bullied in sporting teams, libraries, shopping centres, public transport, even the family home. A "whole school approach" to bullying is only effective to the extent that the bully and the victim are both in the same school.

Schools are a focus point of a child's community, even if they are not necessarily the venue for bullying. Children spend more time in the care of teachers than just about anywhere except the family home. Teachers have long-term relationships with children, and are able to notice changes in their behavior over time.

Programs should be developed for teachers, to enable them to recognize the behavioral changes exhibited by a bullied child. If the child is hiding the abuse, a skillful approach will be required to maintain rapport with the child while teasing-out the details needed to stop it.

Rather than a "whole school approach," what we actually need is a "whole society approach." The school's role as a focus of the child's community should be developed into a nexus for the entire community. **Formalized arrangements should be developed between schools to cater for bullying separated by distance,** so that a coordinated approach can be taken by both places when a bully is in one school and the victim is in another. Awareness campaigns could be developed to inform the wider community that any discovery of bullying in any part of society can be handled discreetly, skillfully and effectively by reporting it to any school. **Consideration should be given to extending mandatory reporting obligations to include bullying.**

This isn't a "cyber" issue. If the Government believes it's a major problem in society, then a major society-wide approach should be used to fight it.

Analyzing information on achieving and continuing world's best practice safeguards

World's best practice is to treat online problems identically to their offline equivalents, rather than banning murder on Thursdays.

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

There is no value in establishing an Online Ombudsman: Who would possibly listen to them?

Consider the regular *panic du jour*, Facebook. Egged-on by the media, Australian politicians fall over each other to out-do each others' overreactions every time Facebook shows up in the headlines. All a prankster needs to do to guarantee themselves a few days of merry media mayhem is use a false identity to create a page on Facebook to denigrate a pre-teen car crash victim. Politicians can't help themselves, disproportionate overreactions are now a "conditioned response."

Enter the Online Ombudsman: Flooded by complaints from Aunt Gladys from Cootamundra, the Ombudsman would investigate, then don a sombre suit and a serious facial expression to duly intone, "I demand that Facebook take down the page."

Facebook, a US company in US jurisdiction operating under US law and not caring one whit about Australian moral-panics, refuses. Now what?

There is no point having an Ombudsman if the Ombudsman has no authority. It is literally impossible for an Australian Ombudsman to have any authority whatsoever over the internet.

The story doesn't change if Facebook chooses to cooperate: The hypothetical prankster could equivalently use (say) *4chan* or *Encyclopedia Dramatica* instead, or any of thousands of other international venues which take delight in treating Australian regulators with outright, demeaning contempt.

If the Australian Government wishes to set itself up for continual impotent embarrassment about the ineffectiveness of its online regulation regime, it can feel free to establish an Ombudsman.

However, failing that, **it makes very little sense to canvass the creation of an Ombudsman that's totally unique to Australia in the same "terms of reference" document that indicates an interest in "world's best practice."** One cannot have it both ways: World's best practice means adopting standards that are consistent across the world, not branching out on a limb that no other jurisdiction has seen fit to climb on to.

Closing remarks

If the public reaction to the ALP's toxic ISP censorship scheme has taught the Government anything, it should be that there is a large subset of the Australian online population who simply doesn't trust the Government to do the right thing online.

It hasn't mattered what the Government has said about their proposal, the key message the electorate has been sending back is, "Yes, that's fine for now, but what about tomorrow when you panic, overreact, and tighten the screws on your censorship system?"

Regardless of assurances about the limited scope of the scheme, everybody knows that in relation to the online environment the Australian Government is a chaotic, fearful, untrustworthy entity who, in the long term, will always err on the side of excessive control. It's built into the Government's DNA, a reputation established over the course of many years, so uncontroversial that it isn't up for debate anymore.

This mistrust hasn't just sprung up from nowhere, it's been earned. The history of Governmental responses to the internet is best characterized as a cacophony of dismal failure, a long parade of poorly-targeted, useless initiatives championed by out of touch politicians who don't know what they're talking about.

Internet censorship. Big red buttons. Websites that crash with the slightest provocation. eSecurity initiatives that attempt to make everyone except end users responsible for end-user behavior. A House Cyber-Security Committee that wastes the valuable time of expert witnesses by quizzing them about fabricated Hollywood movie plots, and recommends mandatory industry codes to force ISPs to respond to security threats which were obsolete years ago. A Government anti-spam body which has made precisely *zero* difference to the amount of spam received by Australians. Content regulation which forces the ACMA to make reprehensibly foolish decisions, turning what should be a prestigious, respected regulator into a finger-wagging, tut-tutting grandmother. Shoehorning ISPs and websites into the same Act of Parliament which regulates broadcasters, even though ISPs are more like the postal service, and websites are more like homes and businesses. A Minister who is pilloried for "spams and scams coming through the portal," and who insists that the Government isn't interested in restricting freedom of speech on the very same day that ACMA blacklists an anti-abortion advocacy site. Kevin Rudd's $120,000 website. The Government's reprehensibly ignorant attacks on Google. Statements by MPs such as those made by the Hon. Maxine McKew, MP during her recent appearance on the ABC's Q&A program, where she made the outrageous suggestion that the internet should be regulated like a newspaper rather than like a water-cooler discussion. An approach to online copyright which legally encumbers the regular, day to day activities of millions of end-users, thereby encouraging a society-wide disrespect for copyright law. Public consultations yielding over 50,000 responses in favor of the establishment of an R18+ rating for computer games, put on the back-burner because, apparently, 50,000 responses is inadequate and more consultation is required. Former Prime MInister Kevin Rudd's ignorant use of the made-up term "band speed" to describe what the NBN will deliver to 90 per cent of Australians. A merry parade of politicians who would be lynched if they didn't know the difference between interest rates and inflation rates, who see no shame in confusing "megabits per second" with "megabytes."

This Government has literally no idea what it's doing with the online environment, and has shown an outright refusal to be educated about it. Is it any wonder that so many people distrust them?

This Committee represents a very rare opportunity to inform the Government. For all of our sakes, I hope they're prepared to listen.