INSPECTING THE DESPICABLE, ASSESSING THE UNACCEPTABLE

PROHIBITED PACKETS AND THE GREAT FIREWALL OF CANBERRA

David Vaile, *University of New South Wales Law Faculty*
Renée Watt, *University of New South Wales Law Faculty*

At first glance the Australian Government's 2008 proposal to install a two-layered mandatory Internet 'content filtering' regime at ISP level – rather than the current opt-in filtering at the user's personal computer – appears relatively straightforward, with a clear mandate, solid unobjectionable aims, little change from existing legal principles and governance frameworks, and challenging but achievable technical goals. Closer inspection does not sustain this appearance; each of these conclusions is shaky; and there are as many interpretations of what is really at stake as there are observers. This paper explores some of the issues that complicate policy development and technical assessment.

> *I cannot forecast to you the action of Russia. It is a riddle, wrapped in a mystery, inside an enigma: but perhaps there is a key. That key is Russian national interest.*
>
> — Winston S. Churchill, radio broadcast, 1 October 1939

1. INTRODUCTION

Australia stands on the historic brink of becoming the first liberal democracy to legislatively mandate Internet content filtering. As a cultural phenomenon, the Internet has generally supported freedom of communication. Filtering proposals sit unhappily with these traditional expectations, and have thus triggered legal, ethical and cultural debates both abroad (Bambauer 2008a; Office of the Privacy Commissioner of Canada 2009; Watt and Maurushat 2009) and locally (Bambauer 2008b). ISP-level filtering promises governments and others the ability to effectively and invisibly enforce decisions about which content citizens may not read or view (censorship) through means of technology or 'code', rather than through traditional legal and administrative action in the physical world. As we observe the dawn of this new era, it is crucial we consider the changes afoot, and how any claimed benefits may weigh against risks or costs.

Lindsay et al (2008) set out the Australian regulatory regime for most forms of content in most media, so this review of issues arising from the Australian proposal for regulating access to global Internet content by means of a mandatory filter at ISP level proceeds from where those authors conclude. Neither a legal interpretative exercise nor detailed technical review, this paper instead signposts some of the proposal's key parameters, describes its interaction with existing regulatory models, and surveys some of the unresolved technical and policy issues. We inspect the Government's mandate, to better understand and assess its proposal; we also consider the significance of the shift away from the enforcement of censorship at the hands of legislators and regulatory bodies, toward remote control enforcement online on an entirely technological level.

EBB AND FLOW OF THE CENSORSHIP TIDE IN AUSTRALIA

The current ISP filtering proposal does not appear from nowhere. There are both historical parallels and continuity with more recent events.

There is a history of expansion and contraction of censorship of new media in Australia. In particular, the small but well-organised pro-censorship lobby consistently seeks to extend censorship (Wallace 2009).

This may be a reflection of international influences such as the long-term struggle in the US, especially around the *Child Online Protection Act* (‘*COPA*’) which sought, similarly to the initial Australian proposal, to render the Internet completely ‘safe for children’. The US Supreme Court ultimately rejected the final version of the *COPA* on constitutional grounds early this year (AFP 2009) after decades of litigation and legislative efforts. But there are local sources as well.

‘In 1956 the Film Censorship Board was established in Australia under the *Customs (Cinematograph Films) Regulations* as a statutory Board whose role was solely to classify films and, from around 1980, video tapes’ (Graham 2000). Its head, the Chief Censor, also later became head of the new the Office of Film and Literature Classification, a non-statutory office within the Attorney-General's portfolio with expanded ambit. More recently the functions were brought more closely under the Attorney General’s Department as the Classification Board and Classification Policy Branch.

Fiona Patten of the Sex Party (an entity largely emanating from the sex industry) recalled in NSW Parliament House in April 2009 (Maher 2009) that Don Chipp, Liberal-Country Party government Minister for Customs responsible for censorship in 1970, caused parliamentary upset by making public the list of banned publications and movies, until then apparently secret.

It appeared from this list that some of the items were of relatively limited offensiveness by the standards of the day, and a number were removed. Many decades later a blog contributor remembered this on the occasion of Don Chipp’s death: “His rulings against the Liberal Party's icy approach to censorship [were] a breath of fresh air. Overnight, we Australians were being treated as adults and not as pupils at a Sunday church school. Unfortunately the current climate is reverting to those dark ages again” (SMH Online 2006).

In the current proposal, it seems the tide of censorship may be coming in instead of going out, and with no latter-day Don Chipp to order the list into the open. The secrecy of the modern black list stems from arguments that would not be persuasive were the filter successful, as there would then be no need for secrecy; but there is no proposal to reverse the statutory change that puts the list beyond *FOI*.[1]

However, there are claims of significant opposition to the filtering proposal, including from a number of Young Labor state branches (Bingemann 2009), and doubts about Parliamentary support in the event that legislation is required (Hansard 2009b), so there seems likely to be at least further vigorous debate.

CURRENT INTERNET CONTENT REGULATION IN AUSTRALIA

Just as censorship across Australian offline media is an historical fact, so too is the fact of Internet censorship old news in the Australian legal dialogue. Schedules 5 and 7 of the *Broadcasting Services Act 1992* (Cth) (‘*BSA*’) already prescribe a complaints-based take-down system for local material or links (Lindsay et al. 2008). Following a complaint, the Australian Communications and Media Authority ('ACMA') decides whether, in its opinion, the Classification Board would, were the content in question to be Classified by the Board, be likely to be given a particular classification from RC to certain MA15+. (See Section 3., below, for more detail.)

If the content emanates from an Australian host, ACMA can issue a take-down or service cessation notice. If the content is accessible via a link on an Australian site, ACMA can issue a link deletion notice.

Within Australia the ACMA's powers are extensive. Hosts have little option but to respond to its notices.

By contrast, content hosted outside Australia – that is, the majority of Internet content – is beyond this kind of direct control. Enter the current proposal, building on the earlier model introduced with the support of Senator Harradine. The aim here is to provide the Australian Government with the means of more effectively censoring its citizens' access to Internet content outside of the Australian jurisdiction. The current system, based on a voluntary decision to use a filter at the end computer level, does not support this.

2. ELEMENTS OF THE PROPOSAL

The Australian mandatory ISP-based Internet content filtering proposal – aspects of which were known as 'Clean Feed', the branding given to a different system in the UK – is a moving target, whose key elements remain elusive. Most official documents have survived as originally released in late 2007 and early 2008, but these too contain ambiguity or silence about specific goals, and official commentary has subsequently brought some of the initial aspects of the proposal into doubt.

This paper will generally refer to the proposal as originally described, and note subsequent variations where necessary.

There are scant references to the proposal – either in general terms or with respect to its aims in particular – on either the ACMA or the Department of Broadband, Communications and the Digital Economy ('DBCDE') sites. Documentation of the so-called 'Live Trial' does provide some insights (DBCDE 2008a; DBCDE 2008b; DBCDE 2008c; DBCDE 2008d). Some of these are singularly unhelpful. For example: 'the purpose is to explore a number of filtering implementation models in order to inform government policy'. This lack of specific aims seems tailor made to facilitate changes to those 'aims'.

The proposal may continue to change after publication of this article, so readers are advised to monitor other sources, such as those mentioned in our references page (Vaile 2009), as well as ACMA, DBCDE and ministerial sites.

TWO LEVELS

The proposal calls for a two-layered mandatory Internet content filtering regime at ISP level.

A. MANDATORY ACMA BLACKLIST FILTER

The first level is a mandatory filter, which will employ a list of Internet Web sites, or page addresses, that ACMA maintains as the 'blacklist'.

The list will be largely fixed (albeit subject to regular or irregular editing), and will range in size from 977 entries in April 2009 (Hansard 2009b, 101) to up to about 10,000 (as required in the filter trial) (DBCDE 2008d). Each ISP will presumably operate from the same list (Brooks 2008).

At the time of writing, the mandatory nature of the ACMA blacklist has come under review, with suggestions that a 'voluntary' ISP Code requiring filters meeting prescribed criteria to be used by all ISPs might replace a legislated mandate (Hansard 2009b; Harrison 2009; Colley 2009). It is unclear if this is in response to repeated indications of lack of parliamentary support from both Opposition and minor parties in the Senate (Hansard 2009a) for a model based on the original proposal.

This paper briefly touches on issues associated with the industry 'Code' scheme in the section dealing with governance issues below.

THE SECRET ACMA BLACKLIST

The epithet 'secret' accurately describes the ACMA blacklist. The *Freedom of Information Act1982* (Cth) ('*FOIA*') administers public access to Government documents. As its title suggests, its aim is 'to extend as far as possible the right of the Australian community to access to information in the possession of the Government of the Commonwealth' (*FOIA* s 3). But a special amendment has specifically exempted the filter blacklist from access applications under the *FOIA* (Communications Legislation Amendment Act (No. 1) 2003). The result is that applicants such as Electronic Frontiers Australia cannot employ the *FOIA* to access the blacklist's content.

The amendment was one of several that effectively exempted from request under the FOIA certain 'Internet-content documents' about 'offensive Internet content' and curtailed access to these documents made by the Australian Government Solicitor ('AGS'), the ACMA, the Office of Film and Literature Classification ('OFLC') and its successors the Classification Board or Classification Review Board under a power in Schedule 5, later including Schedule 7, of the *Broadcasting Services Act 1992* (Cth) ('*BSA*').

The initial version of the list was to be the same as that provided to filter suppliers under the *BSA*. As mentioned above, this list is based on complaints concerning online content, and subsequent decisions that the content is 'prohibited' (made by Classification Board, rare) or 'potentially prohibited' (made by ACMA officers, the majority).

The Minister has indicated variously in March and April 2009 that instead of this list of 'potentially prohibited content', a new list consisting of content that 'almost exclusively' (Brockie 2009) or 'exclusively' (O'Toole 2009) meets the Refused Classification ('RC') definitions – rather than the much larger category that meets the '(potentially) prohibited' definition (RC, X18+, and some R18+ and MA15+) – will form the basis of the blacklist (Conroy 2009; Moses 2009b). Although the nature of the list has apparently undergone variation, the Government has not updated its original documentation (Newton 2009). In the result, not only does the list's content remain secret (because exempt from the *FOIA*), but its criteria remain equally nebulous.

So, as it stands and to the best of our knowledge, the blacklist is primarily based on complaints, mostly from Australians, and subject to ACMA's investigation and de facto classification against a '(potentially) prohibited standard. ACMA may also accept advice from external law enforcement or self-designated child pornography detection organisations (UK Internet Watch Foundation 2008). One would expect that this latter input is more likely to result in serious child porn entries, although the proportion of these caught by IWF is unknown.

There seems to be no planned, large-scale Australian program to continuously and exhaustively 'classify' the Internet, as would be necessary were the list to include even a tiny proportion of the RC or wider 'potentially prohibited' materials accessible on any given day.

The size of the web, let alone the rest of the non-http protocol Internet, is massive. "Even after removing those exact duplicates, we saw a trillion unique URLs, and the number of individual web pages out there is growing by several billion pages per day." (Alpert and Hajaj 2008). The Google index contains only about 40 billion URLs, or 4% of their estimate of total web size. Even if the Google estimate is an order of magnitude or two out, it means there could be tens of billions of pages, with up to a billion turning over or appearing each month. It is known that of the small proportion of child porn which exists on the plain web (almost certainly all RC), much is hosted surreptitiously and temporarily by 'fast flux' insertion or other technical breaches (Watt and Maurushat 2009). There is a vast amount of material likely to meet lesser classifications down to MA15+, which in many countries does not require a restricted access system, and would hence fail our test. Hence it seems likely that either an RC-only list or a 'potentially prohibited' list that attempted to be comprehensive would need repeated and massive sweeps and assessments of immense numbers of sites.

The potentially broad scope of 'prohibition' in Australia and the extremely limited detection ambition in practice carries with it, if implemented, the risk to disappoint the filter's supporters (such as parents hoping it would indeed filter out all 'prohibitable' material – the magic bullet dismissed as wishful thinking by IIA (2006)), because it would be almost certain that the overwhelming majority of those items or pages meeting the Classification criteria to be 'potentially prohibited' material would not in fact be on the blacklist.

This raises questions about the seriousness of the intent at the ISP filtering model's inception: 'success' can only arise if the success criteria do not include actually blocking any but the tiniest proportion of the target category of international web content.

Conversely, if the original aim of blocking 'potentially prohibited' materials represents the agenda, then a Government or other proponent may potentially employ the predictable failures of such a list to call for more resources to complete the task. This is an effectively open-ended request with near certainty of non-fulfilment.

B. 'VOLUNTARY' OPT-OUT DYNAMIC FILTER

The filter at the original proposal's second tier, at one stage called 'Clean Feed', would not be mandatory. It will be 'on by default', but voluntary to the extent that the end user can opt-out. As an opt-out system, the second tier will block users who do not self-nominate as a person seeking exemption (requiring a list of such self nominees), rather than an opt-in system, which would require no action or listing of those seeking to retain an unadulterated feed (beyond what the underlying mandatory filter would block).

The blocking criteria are open-ended, potentially dynamic as well as fixed, and possibly different for different ISPs (perhaps based on a different supplier, or a different specification of block criteria). It is difficult to tell how many items might be caught by such a filter. The filter that at least one House of Australian Parliament employs has about 32,000,000 items on it, according to Liberal Senator Cory Bernardi (Carlisle 2009). The NSW Department of Education filters tens of millions of URLs (Beveridge 2009). These presumably use a combination of dynamic filters and much larger fixed known block lists.

Issues arising from this level of the initial proposal are further discussed below.

THE TEST PROGRAM

At the heart of the current proposal lies a test program (ACMA 2008b; ACMA 2009a), which builds on earlier test programs outlined in reports (ACMA 2007). The Department Broadband Communications and the Digital Economy has described the objective of the test program as follows:

To the extent possible, the aim is to test a range of different types of filtering including:

- ACMA blacklist filtering only (for a blacklist of up to 10,000 URLs); or
- ACMA blacklist filtering plus the filtering of other content using different approaches to filtering which would, for example, include:

    Index filtering of different sized blacklists;
    Dynamic analysis filtering;
    IP versus URL filtering;
    DNS poisoning (DBCDE 2008a, cited in Brooks 2009)

It is beyond the scope of this paper to review the test program or results to date in detail. However, a key issue with the program is the extent to which a clear policy purpose is absent, apparently being deferred until the program produces results (Hansard 2008b). There is a suggestion that the aims, scope and goals of the filtering proposal will be determined by the test outcomes, rather than the test outcomes validating proposed solutions to known aims. Standard IT project planning 'tests' assumptions all the way along, but normally in pursuit of a known goal with explicit or implied scope limits. With respect to the internet filter trials, the question naturally arises: for what is the Government testing?

Senator Conroy expects to receive the results of the test in late July or early August 2009 (Colley 2009).

AIMS?

As noted above, one of the proposal's more opaque aspects is its specific aim. It is easy to see in political terms that there may be some support for a general attempt to 'protect children' from bad things on the Internet (Hansard. 2008a).

However, the translation of this idea into both law and technology with specific functions, costs and risks demands a higher level of specificity. This is particularly important in identifying unintended consequences, which could impose considerable costs.

Seminars hosted by the Cyberspace Law and Policy Centre, the Internet Society and others have generated questions concerning the proposal's specific aims. In particular, which of the following increasingly broad descriptions most closely match the actual aims of the proposal?

- only to avoid inadvertent or unintended viewing, only of child pornography materials, and only while surfing the Web (and in the Flood and Hamilton 2003 version, only by young people);

- to also prevent, detect, block, and help prosecute deliberate access to, publication or circulation of only child pornography or child abuse materials, using the Web and possibly other Internet methods, whether by young people or by adults; or
- to block and detect young people and adults in both inadvertent and deliberate interaction with a wider ambit of 'illegal', 'prohibited' or otherwise deprecated material using any Internet method.

The conflation of these potential but different aims remains at the heart of the puzzle of the Australian filter proposal. This ambiguity with respect to the proposal's aim in part explains its shifting scope and explanations.

When assessing the practical intent of various filtering options, it may be helpful to keep these three possible aims in mind.

LABOR POLICY 2007: WHAT DID THEY PROMISE?

In the later stages of the 2007 election campaign, the Australian Labour Party ('ALP') released a policy document referring to Internet filtering (Conroy 2007). This document remains the immediate source of the current proposal. It describes a policy that had its germination at least a year before (IIA 2006). The policy refers only to one technical document, an undated DCITA file which, like many key Australian Government documents in online policy over a year or so old, is no longer accessible. It cites media and ABS references to a range of harms, namely:

- "online identity theft;
- cyber-bullying;
- abuse of child avatars in virtual worlds;
- computer addiction;
- an increase in the number of registered profiles of sex offenders on MySpace; and
- online breaches of privacy such as the posting of sexual photos and sex videos by students" (Conroy 2007, 1).

A mandatory blacklist filter of 'prohibited' or 'potentially prohibited' content will address few if any of these concerns, since such matters are unlikely to result in an actual or deemed classification of a page or site as 'prohibited'. Nonetheless, the Labor Party document explained the filter proposal thus:

> "Labor recognises that cyber-safety today is an important part of children's overall health and well-being, yet it is one that is not being adequately addressed by the Howard Government. That is why Labor will:
>
> • Provide a mandatory 'clean feed' Internet service for all homes, schools and public computers that are used by Australian children. Internet Service Providers (ISPs) will filter out content that is identified as prohibited by the Australian Communications and Media Authority (ACMA). The ACMA 'blacklist' will be made more comprehensive to ensure that children are protected from harmful and inappropriate online material" (Conroy 2007, 2).

The mandatory policy appears here to refer only to 'homes, schools and public computers that are used by Australian children'. After the election, however, it became clear that the proposal was for all computers in Australia, not just those that children use.

Again largely without referring to any matter susceptible to a '(potentially) prohibited' blacklist filter, the harms for young people were framed as follows:

> "Australian children have increasingly faced online issues such as:
>
> - having their identities appropriated by others;
> - having photos or videos of themselves published online without their permission;
> - suffering from computer and/or Internet addiction;
> - being traced by strangers from details they have entered online;
> - being the subject of cyber-bullying;
> - picking up a virus or Trojan or being the victim of a phishing attack; or
> - inadvertently downloading illegal content when file-sharing" (Conroy 2007, 6).

Among the list of statistics included in the policy document there was but one item with filter potential:

> "Recent Government research shows that:
>
> - 46 per cent of Australian children worry about online safety;
> - 28 per cent of Australian teenagers have seen evidence of online bullying abuse;
> - *38 per cent of Australian children under the age of 13 have purposefully visited websites they think their parents would disapprove of them visiting* [italics added];
> - 24 per cent of Australian children are concerned about pop-up ads; and
> - 17 per cent are concerned about contracting viruses during their online activities".

It is not clear what might comprise web sites receiving parental disapproval' they think their parents would disapprove of', as a range of personal reasons likely provoke such a response. In some instances parents' concerns may overlap with Labor's, such that a filter of 'prohibited' material under the Classification Scheme may allay their fears; however there remain many sites that may be unwelcome for other, unidentified (and non 'prohibitable') reasons.

The then Labor Opposition faulted the former Government on two filter related issues:

> "Some of the deficiencies in the Howard Government's approach are:
>
> - implementation of an $84.8 million PC-filtering program, where the filters are easily bypassed and rendered ineffective, as was demonstrated in August 2007 by a 16 year old school boy; ...

> • the current ACMA blacklist under the Howard Government is inadequate. It does not contain enough sites to protect our children from *harmful and inappropriate content*" [emphasis added]; (Conroy 2007, 4)

The document went on to repeat the ISP filter proposal in a little more detail:

> "Mandatory ISP Filtering
>
> A Rudd Labor Government will require ISPs to offer a 'clean feed' Internet service to all homes, schools and public Internet points accessible by children, such as public libraries.
>
> Labor's ISP policy will prevent Australian children from accessing any content that has been identified as prohibited by ACMA, including sites such as those containing child pornography and X-rated material.
>
> Labor will also ensure that the ACMA blacklist is more comprehensive. It will do so, for example, by liaising with international agencies such as Interpol, Europol, the Federal Bureau of Investigation (FBI) and the Child Exploitation and Online Protection (CEOP) Centre and ISPs to ensure that adequate online protection is provided to Australian children and families" (Conroy 2007, 5).

Again this seems to clearly indicate that the intended audience for the filter was 'children', not everyone. Given this background, it is small wonder that the extension after the election to *all* users has caused considerable controversy (media references in Vaile 2009).

The policy was expressed so as to "require ISPs to offer" filtering. The language had connotations of the end user having some choice about whether to respond to this offer. This policy text clearly appeared to fall short of requiring ISPs to supply nothing else, unless perhaps it is "an offer you can't refuse".

This section of the document also referred to 'child pornography and X-rated material'. The former constitutes RC-rated material. Together these two matched the then extent of '(potentially) prohibited content' under the *Broadcasting Services Act* (Lindsay et al. 2008) which, as explained above, forms the basis of items which might be on the proposed blacklist, if subject to complaint.

But, at that stage, Parliament had already passed amendments (Communications Legislation Amendment (Content Services) Act 2007) extending the scope of the '(potentially) prohibited' category, below X-rated material to include some MA15+ and R18+ material. This significantly broadened the scope of filterable material into for example, the realm of material broadcast on late evening television, and including a lot of 'legal' heterosexual and gay pornography falling short of X or RC ratings.

The ALP Election Policy gave no specific examples of the range of targeted material, nor any indication that the scope of 'potentially prohibited' on the Web was to suffer dramatic expansion after the election. The policy gave the impression that the target material was confined to X-rated or RC material when, in reality, by January 2008 '(potentially) prohibited' would be much broader.

Thus, in addition to the scope creep of the target audience, as explained above, from children to all adults, there has since the announcement of this policy also been scope creep in the range of banned materials beyond the initial RC and X-rated material. Consequently, the plan became much broader, including less objectionable material than that which featured in the original proposal.

SCOPE CREEP AND THE MANDATE

'Scope creep', meaning the uncontrolled extension of goals and tasks that are 'within scope' is acknowledged as a major cause of project failure and risk manifestation for large scale IT projects. The online and software industries fail to meet project management success criteria in a large proportion, often a majority, of projects affected by scope creep (McConnell 1995). Scope creep under the ISP filtering proposal is therefore a very real concern, even from a narrow technical perspective. These technical issues are taken up further below.

ISP-level filtering's scope creep also raises governance concerns about the extent of any electoral mandate provided under such a policy: are the policy scope changes that have occurred significant enough to raise questions about what the voters thought they were getting?

CONTINUITY WITH SOME COALITION POLICIES

Despite the new Rudd Government's statements in 2008 criticising the policy of the previous Howard government, there has been a significant degree of continuity between the two approaches, particularly in relation to the ISP filtering model. The previous Government, in fact, implemented the testing of ISP based filtering, and produced a report of the results (Coonan 2007a, Coonan 2007b).

It is arguably better for public policy for governments to acknowledge the extent of such continuity, so that policy makers can objectively discuss precise changes in proposed solutions.

DISPUTED IMPLICATIONS OF LOW NETALERT TAKE-UP RATE

One area where there has been a clear difference between Labor and Liberal policies is the voluntary NetAlert PC-based filter scheme. The NetAlert scheme was a product of the Howard Government. The new Government, however, has condemned the low take-up rate of NetAlert PC-level filters as an indication of failure, and on 31 December 2008 ceased to provide free PC filters to new applicants.

Data updates for the existing users of PC-level filters were to be maintained (Australian Government 2008, FAQ 15). Nevertheless, the take-up rate in Tasmanian trials was quite low, under 10% and typically under 5%, averaging 3% (ACMA 2008b). The low take-up rate, and the reported breach of security by one young person, appear to have discredited the PC-based filtering model in the eyes of the Labor Party.

Factors apart from the perceived effectiveness of PC-level filters may, however, lie at the heart of a low take-up rate. Opponents of filtering suggest that ambivalence toward NetAlert represents the true level of market demand for Internet filtering. On this view the Tasmanian trial is a repudiation of popular interest in Internet filtering, and not a reflection of a desire for more effective filtering.

At least two factors complicate such an interpretation. Firstly, the filters can be complex to install for a technically naïve person (perhaps a typical parent). Secondly, the successful hack of the system by a young person received extensive publicity. This appears to have prompted the (probably inaccurate) belief that children could easily bypass the system.

3. MANDATORY BLACKLIST AND CLASSIFICATION ISSUES

WHY IS CLASSIFICATION RELEVANT TO THE FILTERING PROPOSAL?

The ISP Filtering policy's mandatory blacklist contains material that must meet the criteria in the *BSA* for potentially or actually prohibited content. This means that for the first time in Australia, Parliament is proposing a technological means to apply statutory criteria to the interception and blocking of messages and transactions on the Internet or other communications devices. This is an historic proposal.

The unprecedented nature of the proposal aside, another striking feature of the ISP Filtering proposal is that the confused matrix of Australian censorship now applies much more stringent standards to online material than to films or literature or, indeed, to any other off-line content. This is contrary to various stated intentions to treat online material the same as it would be offline.

WHAT IS THE BASIS OF CENSORSHIP CLASSIFICATION GENERALLY IN AUSTRALIA?

The Australian censorship scheme involves a system of classifications under the National Classification Code. The scheme is based on provisions in Commonwealth instruments including Classification (Publications, Films and Computer Games) Act 1995, Classification (Publications, Films and Computer Games) Regulations 2005, Guidelines for the Classification of Films and Computer Games 2005, and Guidelines for the Classification of Publications 2005.

Lindsay et al. (2008) and Watt and Maurushat (2009) set out details of the complex scheme of censorship classification generally in Australia.

Notably, there is no reference to online or Internet content in any of these schemes. Internet content exists outside the traditional statutory categories, and is rarely actually classified.

Where subject to classification scrutiny, Internet and other online content is, strangely, usually treated as if it were a form of cinema film, even if the material is predominantly textual.

CLASSIFICATIONS AND INTERNET CONTENT

Table 1 sets out how various classifications map against material of various types. The first three columns below are based on the table in Griffith (2009), with the remainder extrapolated from the BSA and other laws. See also the *National Classification Scheme* (Classification Policy Branch 2006, 9).

Internet content and links to Internet content, like certain other electronically-accessible material such as 'mobile premium content', are not subject to a separate clearly identified statutory censorship classification regime administered primarily by the Classification Board but, instead, to a scheme run by ACMA based on existing classifications to determine what is meant by 'Prohibited' or 'Potentially Prohibited' content.

"Prohibited content" under the *BSA* is content which has been formally classified by the Classification Board into certain classifications. Material not classified by the Classification Board will be "Potentially Prohibited" (and thus effectively prohibited in practice should the mandatory ISP filter use this *BSA* 'Prohibited' category as the criteria for its block list), if, in the opinion of ACMA, it is likely to be given a particular classification if it were ever to be classified by the Board.

A person seeking to understand the classification schemes for most types of material would typically start with the Classification Board. However the Classification Board's site (Classification

Policy Branch 2006, 9) makes no substantive reference to either "online content" or "Internet content", unlike its detailed explanations of all the other types of material which is subject to censorship classification, and it is thus of limited assistance to anyone seeking to understand how Internet content is classified. There is more information on the ACMA site (ACMA 2008e; ACMA 2008f; ACMA n.d.a; ACMA n.d.b; ACMA n.d.c), although this does not seem to have been clear enough to ensure that the debate about the proposed ISP-level filter started from the knowledge that, from January 2008, 'Prohibited' material on the Internet and mobile communications platforms in Australia can mean certain MA15+ material as well as R18+, X18+ and RC.

The operation of various provisions of the *BSA* (Schedules 5 and 7) creates a *de facto* statutory model for online and digital content based upon, but different in some key respects to, that applying to most other material. The 'Online content' column in the Table attempts to extract the effect of the existing model as applied to Internet content.

Publications *	**'Films'**	**'Computer Games'**	**Online 'eligible electronic publication'**	**Other online or mobile content**	**Criminal to possess, access: "illegal" ?**
Unrestricted	**G** General	**G** General	**Unrestricted**	**G** General	
	PG Parental Guidance	**PG** Parental Guidance		**PG** Parental Guidance	
	M Mature	**M** Mature		**M** Mature	
	MA15+ Mature Accompanied	**MA15+** Mature Accompanied		**MA15+** Mature Accompanied [some Prohibited]	
Category 2 restricted	**R18+** Restricted	**RC** Refused Classification	**Category 2 restricted** [Prohibited]	**R18+** Restricted [some Prohibited]	
Category 1 restricted	**X18+** Restricted	**RC** Refused Classification	**Category 1 restricted** [Prohibited]	**X18+** Restricted [Prohibited]	
RC Refused Classification	**RC** Refused Classification	**RC** Refused Classification	**RC** Refused Classification [Prohibited]	**RC** Refused Classification [Prohibited]	[**Some**: child pornography/ child abuse]

Table 1 Classification schemes for different types of material
*'Publication' categories do not match the set used for for films, AV material and computer games, or online content. Online or mobile versions of certain paper publications (or audio recordings thereof) available in Australia are treated as 'eligible electronic publications', classified as if publications, but all classifications except Unrestricted are subject to the 'Prohibited' or 'Potentially Prohibited' online content category model in the Broadcasting Services Act Schedule 7. TV broadcasts are based on a variant of the Film scheme.
The shading indicates categories subject to the most vigorous suppression available for that type of material. In some cells (MA15+ and R18+ in the online column, RC in the criminally sanctioned material column), only part of that classification is subject to the most vigorous suppression.
(Guidelines for the Classification of Films and Computer Games 2005; National Classification Code n.d.)

The IIA *Content Services Code* does set out a system for applying Classifications to Internet content (IIA 2008; see also Collins et al. 2008).

Under the *Content Services Code*, the first principle is that "as far as practicable and consistent with regulatory requirements, there should be 'electronic equivalence' – that is, behaviour and transactions that can take place in the physical or paper-based world should be permissible over digital delivery technologies without additional requirements or restrictions" (IIA 2008, para 3.1). It appears from Table 1 that this principle is unlikely to be viable in practice, since the effective scope of online and mobile content 'prohibition' is so much broader than the effective prevention of adult access to content in the other classification schemes, which in its most vigorous form generally only covers RC material (the darkest shaded regions of the table).

Unsurprisingly, from the notification document in a recent sample classification decision (Jacobs 2009a) the Classification Board, hamstrung by the lack of any real categories for Internet content, appears not to have applied a consistent categorisation for online content items it has classified (Jacobs 2009a).

The current Internet classification scheme also draws a fundamental distinction between locally hosted and international materials (BSA 1992; IIA 2008).

Internationally hosted material clearly does not require actual classification. Local online content may be classified, but is rarely if ever submitted for classification and, unlike other content types, need not display a rating. Nonetheless, users may complain to the ACMA about online content. Such complaint results in the ACMA assessing the site, and may also result in classification by the Classification Board ('CB'); this was proposed as the mechanism for listing on the blacklist.

WHAT IS THE INTENDED SCOPE OF THE MANDATORY FILTER?

There has been significant unnecessary confusion about the scope of the mandatory ISP-level filter proposal. For example, on an SBS Insight program on 31 March 2009, Minister Conroy said, in relation to the intended mandatory censorship system, 'we are talking almost exclusively about Refused Classification' (Brockie 2009). In April on ABC Radio JJJ's *Hack* program, however, he appeared to indicate a narrower scope:

> Senator Conroy – "As we've always said, this is about Refused Classification. This is about material that is currently Refused Classification like child pornography, bestiality."
>
> Kate O'Toole – "The stuff on the ACMA blacklist though, that isn't RC, that isn't Refused Classification, the blacklist is broader than that. So are you only going to be –"
>
> Senator Conroy – "We've never stated that we were going to do anything other than Refused Classification" (O'Toole 2009; Newton 2009).

Statements in April and May 2009 by Minister Conroy (Hansard 2009b) indicate a potential distancing from the notion that the mandatory filter will be targeted at the current ACMA blacklist, which must contain material of which ACMA is aware and which it understands to be either 'prohibited' or 'potentially prohibited'. The new formulation has invited the inference that only RC material will be listed, but it did not expressly say as much, as of early June. The boundary conditions for the material that falls short of RC but that will fall within scope of the filter remains disturbingly unclear.

Apparent abandonment of the initial '(Potentially) Prohibited' category as the criterion for the proposed mandatory filter, while welcome in some quarters, creates a number of difficulties. There is at present no statutory scheme describing any other bases for deeming Internet content to be unfit for access by Australian users. It follows that a new legislative scheme will need to be introduced.

The current scheme seems to treat most forms of online content as if it were a film. It would be interesting to see if a new statutory scheme would finally attempt to acknowledge and describe various forms of Internet content, and the differences between such forms, such as a page of text, text and images, images and sound, moving images and sounds, animation, interactive content, collaboratively generated content, and so on. The lack of any description or acknowledgement of the range and nature of Internet content is striking when compared with the extent of the intended censorship, and the detailed treatment of other forms of content. It is possible that a more explicit treatment of different forms of online content may even move to redress the excessive prohibition that has been applied to online materials compared with others.

The statutory extension of prohibition to all commercially motivated MA15+ material not sufficiently age-restricted (effective January 2008, *after* the announcement of the new filtering proposal), received little scrutiny in 2007, when most attention focussed on the novel mobile services aspect of this change. But given the sustained controversy and international interest around the current proposal, legislation introduced in 2009 or 2010 to create a new and different, or additional, Internet content censorship scheme would likely receive more sustained scrutiny.

Unless the Government overhauls the Internet content regulation regime at the same time, the continued operation of the 'prohibited' model would surely be cast into doubt. Its current purpose is to form the basis of a list given to PC-based filter suppliers. If a different and lesser list were given to mandatory ISP based filter suppliers, while they were also encouraged to block a much wider range of "unwanted" material, there would be no obvious application of the category to content outside Australia.

CAN THE MANDATORY FILTER BLOCK OUT WHOLE SERVICES?

While the NSW Department of Education may be able to justify banning blogs, wikis and many other interactive Web 2.0 services in its schools' blacklist (Beveridge 2009), this seems less sustainable for a mandatory filter applied to the whole population.

Yet it seems increasingly likely that rather than individual pages or sections, whole sites or IP addresses will be blocked. This is likely to cement large scale over blocking, because presumably not all pages on a site would offend whatever criteria was involved.

Indeed, the Wikipedia site was blocked because of a complaint to the Internet Watch Foundation (IWF) in relation to one page containing an image of the cover of a decades old record (Moses 2008).

4. OPT-OUT DYNAMIC SYSTEM ISSUES

The second tier of the proposed filtering scheme is a pseudo-voluntary (Annetta 2008) system based on algorithmic dynamic matching, not on matching a simple finite mandatory blacklist. (How dynamic matching works in detail is beyond the scope of this paper.)

This type of dynamic filter may be the real challenge for 'real world' filtering efforts, since this is what would most likely have to deal with the hard cases, namely those where there is no match against a fixed list but there are some risk factors or criteria that trigger some positive and some negative matches.

While the opt-out element of the proposal does provide some benefits for user control, it also presents different problems for governance. This paper discusses this issue only in passing, since most attention has continued to focus on the mandatory aspects of the proposal.

The second tier of the proposed scheme is, nevertheless extremely important. In practice, and will only become more so if for whatever reason the mandatory blacklist is for whatever reason abandoned or restricted in scope, The opt-out system of additional filtering may well constitute the bulk of the items that are actually filtered, since there is so little material on the ACMA black list. As such, and especially as there may be a dynamic component created and destroyed on the fly, this tier represents a much harder system to subject to scrutiny. There may be no 'list' extant outside the operation of a filter algorithm on any particular day (ACMA 2008b). And to the extent that it is left to private businesses to supply and operate, there may be less transparency and participation that with a government system, which at least has to face some public scrutiny one way or another. Fully private 'Code'-based systems can be notoriously difficult for consumer or public interest advocates to engage with, unless this engagement is built into the scheme at the foundation level. While there may be some scope for competition to give users a choice of options, private commercial provision of filtering, especially on a pseudo-voluntary opt-out basis, is inevitably compromised by a lack of transparency, and could create significant cause for concern in its own right.

5. YOUNG PEOPLE'S INTERESTS

Although the filter proposal has been characterised as largely aimed at achieving some benefit for young people (children and teenagers), it is doubtful whether it is a useful approach to addressing the problems of young people online. In particular, there are increasing concerns that the real needs of young people, including varying needs from early childhood to late teens near adulthood, are not being treated robustly enough and with recognition of modern understandings about how to build resilience.

The technical filter model is not necessarily directly compatible with some of the other and perhaps more effective mechanisms for dealing with the uncertainties, risks and opportunities for young people online.

THREATS TO YOUNG PEOPLE ONLINE

To begin with, the problems encountered by young people online are much broader than access to offensive material.

The ALP policy (Conroy 2007) identified a range of security issues for young people. Broadly speaking these can include any of at least the following range:

- stalking
- bullying
- piracy
- gambling
- spam
- malware
- phishing and scams

- temptations of ‘sexting’
- recruitment or grooming for child porn or abuse participation
- exposure to child porn material
- exposure to prohibited content’
- Facebook and the risk of excess self disclosure of personal information/privacy
- information that is disturbing for whatever reason, not prohibited content
- temptation to purchase illegal material
- hate speech and recruitment to vilification
- violent online games, disrespectful of women
- surveillance, censorship and privacy abuses

ACMA’s first report grouped risks into ‘content, communication and e-security’ risks (ACMA 2007, 3). Surprisingly, it did not identify the nature of the content threat, apart from the bare description of ‘exposure’ to ‘illegal or inappropriate’ content. For instance, it failed to indicate the sort of harms or outcomes which are the actual manifestation of the risk, unlike in the other categories where clear negative outcomes were identified.

It is clear that, of the threats identified to young people online, the vast majority would not be affected by a blacklist web filter. Even those such as child pornography, which would be classified ‘RC’, are of marginal relevance, given the very limited proportion of such material that is now likely to be on the open plain HTTP web, as opposed to more secure back channels.

If there were a broader, all ‘potentially prohibited’, focus of the mandatory filter, then potentially it would have some blocking effect on the broader range of material regarded as being unsuitable for children. . But for the reasons given above, relating to resources and a complaints basis for selection, there is very little actual material on the current blacklist which falls into the MA15+, R18+ and X18+ categories. The practical constraints on compiling and maintaining a blacklist, and perhaps also the original list’s motivations from that time when ‘prohibited’, ‘illegal’ and RC were almost synonymous, mean that the list primarily includes ‘RC’ material, and this mostly child abuse material. So the list, unless drastically expanded, would do little to block all the other material outside the RC category.

CHILDREN, TEENAGERS AND PORNOGRAPHY

The policy behind the ISP filtering proposal seems to take as a given that exposure to pornography is disadvantageous for teenagers and children, and that it can be effectively prevented by a filter. Malamuth and Huppin (2005) suggest that while there are some associations between consumption by teenagers and their behaviour, in many cases the most negative impact is only in already highly antisocial or aggressive subjects. Moreover, the wide variability in outcomes makes reliable associations difficult to draw.

It is difficult to predict whether the ACMA Blacklist filter would have any real impact on this issue, since the studies mostly refer to consumption of material that is lower in the classification scheme than the RC category, which apparently forms the basis of the list for the latest (May 2009) version of the proposal. To block the range of material which many studies have canvassed, one would need to maintain, on a continuous daily basis, a filter which was proactive and encyclopaedically complete (and thus extremely resource-intensive and prone to overblocking), rather than the complaint-based and thus more or less tokenistic model proposed.

(It would also need to extend down much lower in the classification scale, to X 18+, R 18+ and probably to the original MA15+ category as well, if not further.)

The open-ended cost of maintaining such a filter as a continuously updated truly effective block, rather than as a token gesture, could substantially limit its attraction, especially in a time of financial crisis.

Furthermore, the underlying question of whether technically blocking such a wide range of material from users would solve an identified and specific problem with teenagers is unresolved. There may be some intuitive attraction to an effective means for restricting such access, especially for younger children, and some efforts in this direction may be useful in certain circumstances. But there is a growing body of opinion which suggest that the range of potential hazards online for a young person becoming an adult extends way beyond what any real world filter is likely to be certain of blocking. This means that the use of a filter may give rise to a false comfort, since children and young people will still be exposed to most of the hazards.

There is also a risk of losing the respect and trust of those blocked behind such a wide and potentially arbitrary censorship filter, and of implying that they cannot be trusted to engage with the wide range of opportunities and potentially beneficial features of the online world without the aid of a technical block on content. This negation of trust is potentially corrosive for the development of independent self restraint, and the capacity to detect and reject dangerous invitations and temptations. The real source of 'protection' is thus less likely to be found in technical blocks than in extensive and well-supported efforts to increase the resilience of young people at various ages, by whatever means are found to work (Graham 2009; Doel-Mackaway et al. 2008; McDougall 2009).

The need for multiple methods of promoting the interests of young people has, in fact, been accepted by government (Conroy 2009). This aim is often characterised as 'protecting' them, but in practice, achieving effective results may require a much more expansive view of capacity building, than a simplistic attempt to restrict access to content.

CHILD PORNOGRAPHY AND CHILD ABUSE MATERIAL

Child pornography and child abuse material is extensively criminalized (Albury, Lumby and McKee 2008; Criminal Code 1999 Qld s228C). The relevant federal offence prohibits a wide range of dealings with "material that depicts or describes, in a manner that would in all the circumstances cause offence to reasonable persons, a person under (or apparently under) the age of 18 years: (a) engaged in sexual activity, or (b) in a sexual context, or (c) as the victim of torture, cruelty or physical abuse (whether or not in a sexual context)." (Criminal Code 1995 (Cth), s474.19). NSW has the age at 16 years (Crimes Act 1900 NSW s91H).

While many aspects of the ISP filtering proposal are controversial, it is widely accepted that an effective response to the separate problem of child pornography is a legitimate matter for law enforcement detection and apprehension of perpetrators (Griffith and Simon 2008).

The nature of the targeted activity is, however, highly secretive, and thus difficult to research. Wikileaks' anonymous German contributor, 'X', claims to provide an inside account of the domain, particularly the business model and technology (X 2009).

Despite agreement on the need to effectively police child pornography, there are reservations about whether the proposed filtering model will be effective against this material, or whether it may, paradoxically, compromise law enforcement efforts. In particular, there are concerns that a mandatory blacklist filter:

a. will not block the channels for child porn, most of which are not on the open public Internet using plain HTTP protocol, but rather on more secure channels including secure HTTP protocols, encrypted news or file transfer, P2P, Tor and other systems; and
b. may even hinder apprehension by driving the business or unwary participants further underground, away from scrutiny and detection.

It should be noted that there have been regular reports of the apprehension of large numbers of members of global child pornography networks, in many cases via inadvertent exposure over less secure channels, and including detection by ordinary web users (ABC 2009; ACMA 2008a).

In late May 2009, anti-filter activists in Germany claim that direct action, namely writing emails to hosts of child porn material deduced from local blacklists is effective in removing child porn sites, or confirming that there is no such material on the site (AK Zensur 2009). The latter false positive problem was also reported from those reviewing the alleged Australian lists leaked to Wikileaks (Moses 2009a; Kravets 2009), but it is not known if the German takedown request initiative and followup has been replicated in Australia.

6. 'TECHNICAL' ISSUES

FRAGMENTATION

As Tim Wu (1999) has pointed out, different application platforms are significantly different for purposes of filtering and censorship. Moreover, new applications increasingly fragment content channels. Ongoing fragmentation of protocols, messages, data streams and secure channels clearly raise implications for filters. Consequently, it seems clear that for determined rather than merely inadvertent engagement with and distribution of deprecated material, a plain web/HTTP protocol filter would be of little use.

In effect this means that a web filter is really only likely to work for inadvertent or accidental access to sites with the most serious material, such as child pornography and child abuse material. The problem is that in this case of child pornography, the most seriously cited issue to be addressed by the ISP filter, it appears that very little of the total Internet traffic in it occurs using plain web sites established for the purpose. Those plain web hosts that do contain child pornography are likely to be compromised by fast flux parasitic malware, injecting the material into obscure locations on legitimate hosts, and removing it again shortly thereafter. This seems to have been the explanation for a Queensland dentist's site appearing on the ACMA blacklist.

As mentioned above, the other modes of distributing child pornography are generally not plain HTTP (Ghosh 2008).

POTENTIAL IMPLICATIONS FOR E-COMMERCE AND SECURITY

End-to-end authenticated channels using encryption and certificates to ensure that no intervention occurs between known and trusted end points are essential for secure e-commerce transactions. They would be difficult for a filtering scheme to crack open, without spoiling the basis of the trust by inserting a ‘man in the middle’, the basis for many malware architectures. This trust is the heart of secure transactions involving currency, amongst other things.

The proposed filtering scheme therefore has potential implications for e-commerce and payment systems, and for any scheme using Secure HTTP protocol (HTTPS) and similar methods for addressing the inherent insecurity of the open Internet (Hanmore 2009). At worst, secure channels are a simple means of bypassing an ISP-based filter.If secure means of communication were compromised by filtering, there would be implications so drastic for e-commerce and e-banking that it could not easily be contemplated.

COMPUTER GAMES

The Classification Board must refuse classification for ‘computer games’ if the content would be rated above MA15+ (i.e. R18+, X18+ or RC) in other media (National Classification Code n.d).

In comparison to content other than computer games, certain Internet content likely to be classified as R18+ would, if characterised as ‘computer games’, be Refused Classification. Australian retailers could not legally sell such games, even with a high standard age verification system (‘AVS’).

Online games could therefore meet the requirement of two statutory content categories, as both ‘computer games’ and as ‘online content’. As online content, R18+ games would not be prohibited (providing a suitably rigorous AVS were in place). If classified as a game, however, such content would be RC, and the AVS would be irrelevant.

Classification of game content in an online environment, where there is not a fixed DVD of closed material but an open-ended potential system of both intrinsic content and user-generated content, is extraordinarily complex and difficult, effectively defying the existing classification categories

VIRTUAL WORLDS AND CLASSIFYING BEHAVIOUR

‘Virtual World’ online social games (for example Second Life, or World of Warcraft), while presently declining in popularity, are potentially problematic ISP content filter targets, since the classifiable content arises from interaction with other characters and avatars, rather than the game’s pre-programmed agents.

In short, it would be much more difficult to classify the ‘content’ in advance, as it is not within the game organiser’s close control. There is little prospect that the standards required of users in the game worlds’ Terms of Use (often drafted in the US or EU) would map conveniently to the complex matrix of the Australian classification system. Moreover, infringements of Australian classification are unlikely to be detectable by the Classification Board. Even if the Board did detect relevant infringements, it is hard to envisage what effective action could be taken to suppress this (Bradley and Froomkin 2006).

In addition, while recent judgments in Australia have suggested that even cartoon figures can constitute “a depiction of a person” for the purposes of liability for child pornography, (McEwen v Simmons 2008) NSWSC 1292, which confirmed a conviction for "offences of 'possessing child pornography' contrary to s 91H(3) of the Crimes Act 1900 (NSW), and 'using ... computer to access child pornography material' contrary to s474.19(1)(a)(i) of the Criminal Code Act 1995 (Cth)) it is by no means clear that either the operators or participants of off-shore virtual worlds would be operating under the assumption that real-world standards of behaviour should apply in-world. This raises serious legal issues. For example, what would the undefinable 'reasonable person' of the Classification Code (National Classification Code n.d.) think of the standards of the game world? Would they apply the standards of their real world community or of the game's community?

After all, part of the purpose of engaging in fantasy and role-playing games may be precisely to escape normal expectations of decent behaviour. The worst violent offences, such as premeditated and unrepentant murder, are a normal and accepted part of many games. While child abuse and child pornography are deprecated and generally unacceptable, 'age play' and deception about one's gender and age are not.

Given the likely difficulty in determining the 'apparent age' of avatars, who are often intended to look young and sexy, the fact that many players are young, and the breadth of the child pornography laws in Australia, it is likely that there may be a significant number of inadvertent or deliberate breaches of Australian classification laws were the Classification Board to apply its standards to virtual worlds. Also, given the unpredictability of player behaviour and the deliberately transgressive and violent intent in many other games, it is equally likely that other breaches will occur around the levels of online game violence.

In these ways virtual world games present a particular challenge to a mandatory blacklist filter. The simple but brutal option of a blanket ban on whole game environments, most of whose play may be compliant with classification at levels below 'RC / prohibited', seems as fraught with problems as the alternative of trying to dynamically classify behaviour in real time. Such difficulties may not of course deter legislators from attempting to regulate behaviour in virtual worlds.

SCOPE CREEP INTO OTHER DOMAINS: COPYRIGHT

As Australia's ISP filtering proposal continues to evolve, the possibility of scope creep into other domains of the ISP-based content filter, once established, remains a live concern. Copyright filtering is an obvious candidate.

Around the world (EU 2007, Horten 2009, Anderson 2007), the entertainment industry has been agitating for governments and ISPs to implement filtering technology to prevent online copyright abuse (Yu 2008).

While websites employ text and images in breach of copyright, the entertainment industry's principal concern lies with peer-to-peer ('P2P') file-sharing, which allows users to connect directly to each other's computers and thereby share music and audiovisual materials. Unless users share such files pursuant to an agreement with the copyright holder, or are themselves the copyright holders, the copying and communicating to the public that is inherent in file-sharing (Sharman case 2005) of 'sound recordings', 'musical works', 'cinematographic films', and 'television broadcasts' will infringe copyright (Copyright Act 1968).

Because P2P technology is discrete from web browser technology, the filtering of each demands different technologies. The Australian ACMA ISP blacklist, operating as it apparently does only against web sites (HTTP protocol), will be ineffective in preventing copyright infringement via P2P, and probably even over secure HTTP.

But the technological inability of the current system to effectively filter copyright materials on P2P does not make such a filter impossible. Formerly the domain of network security, deep packet inspection ('DPI') is fast stepping into the limelight as the technological protégé of the copyright filter brigade (Bermeister 2009). DPI allows the intermediary nodes on an Internet connection to analyse data in transmission ('packets').

Attributes of packets visible to a DPI application include not only the IP addresses of senders and recipients, but, importantly, the source application (for example email, web browser request, P2P). (Parsons 2008) That is, DPI can distinguish between types of Internet traffic. This in turn facilitates the differential treatment of traffic, whereby certain types of packets are a high priority, and so enjoy swift delivery, while others can be throttled. A useful analogy is perhaps the transit lane on Australian roads: certain types of vehicles (those with several passengers) are entitled to use the fast lane, while others remain stuck in traffic.

DPI is the wonder child of copyright filter supporters because it presents the technological opportunity for ISPs to stifle P2P traffic. Both in Europe (EU 2007, Horten 2009) and the US, (Anderson 2007) the entertainment industry is campaigning for a DPI copyright filter.

DPI filtering targeting copyright materials will, however, encounter legal and ethical problems. Firstly, not all P2P traffic is illegal. Were we to ban technology whose principle original purpose involved breaching copyright, we would not have enjoyed such developments as the audio cassette (ATMA v Cth 1993) and VHS: stifling technology with both infringing and non-infringing uses runs counter to any policy of support for technological innovation. P2P clearly has legitimate uses, which should not be outlawed.

Secondly, the notion of traffic shaping is abhorrent to the cardinal rule of communications law: non-discrimination. Non-discrimination of communication stipulates that all communications are equal – that each person's telephone call is equally important, that each user's Internet traffic is equally valid. In application to the Internet, the principle of non-discrimination is also known as 'net neutrality' (because all communications are neutral) and represents the ethos of Internet culture (Ohm 2008; Parsons 2008). Under net neutrality, all communications are equal. DPI, however, brings to mind Orwellian predictions, whereby some communications are more equal than others.

A third reason for concern with DPI is its potential conflict with Australian privacy legislation. The *Privacy Act 1988* (Cth) stipulates that 'an organisation must not collect personal information unless the information is necessary for one of its functions or activities' (s 6, Sch 3 cl 1.1.). Any copyright filter in Australia will probably sit at the ISP level, because ISPs are the bodies that supply Australians with Internet service, and as such represent the most accessible intermediary nodes through which all Australian Internet traffic must flow. As incorporated entities, ISPs comprise 'organisations. As 'collect' retains its ordinary meaning (Seven v MEAA 2004, 45) being to 'gather' or 'assemble', DPI 'collects' data within the relevant statutory sense. Because DPI identifies the IP addresses of a packet's sender and recipient, information which is reasonably attributable to a particular individual, the data collected constitutes 'personal information' (Privacy Act 1988, s 6).

An ISP's function or activity is to provide an Internet connection to an end user. Filtering this connection to copyright materials is neither 'indispensable', nor even 'expedient' to such an activity. Where necessity entails a semantic grey-area between these two values, DPI is clearly not 'necessary' to an ISP's functions or activities (Tenants Union 2004, 49). Also, information concerning users' browsing habits is commercially valuable (and of considerable value for profiling political, moral and other attributes) and therefore 'sensitive', which raises the threshold for necessity (Tenants Union 2004, 49).

The Office of the Privacy Commissioner of Canada has recently expressed similar concerns, in the following terms:

> How does society reconcile the technological benefits and privacy impacts of new technology? Deep packet inspection is just one seemingly neutral technological application that can have a significant impact on privacy rights and other basic civil liberties, especially as market forces, the enthusiasm of technologists and the influence of national security interests grow stronger' (2009).

As powerful stakeholders lobby globally for a copyright filter, the potential for Australia's ISP-level filtering project to extend to this area is cause for concern. This should be recognised as an attempt on the part of the global movie and music industry to externalise the costs of protecting its own economic interests – by instituting filters at ISP level, shifting costs and risks onto ISPs and ultimately end users – and potentially ride on the coat-tails of other filtering proposals.

7. GOVERNANCE ISSUES

A variety of perspectives can illuminate the governance issues associated with the filtering proposal. The governance issues include the importance of proper decision-making, risk and cost/benefit analysis, and participatory process. To begin with, the filtering proposal can be viewed as an example of a large-scale government IT project methodology with uncertain aims. Over and above this, however, it is apparently an exercise in 'evidence free' policy development in the era of 'Evidence-Based Policy' in a controversial and morally-charged domain, in response to passionate advocates seeking to claim the high ground. The combination of these factors, and the ambiguity about goals, creates ripe conditions for governance problems.

DIFFICULTY IN IDENTIFYING STABLE GOALS AND SCOPE

In describing the aims and scope of the ISP filtering project, the Government has employed frustratingly elusive and changeable language, particularly about the specific characterisation of the material to be filtered. While this may be attractive to policy-makers for retaining the latitude for 're-positioning' the message around a project, it is not conducive to effective system design methodology, usability evaluation, risk auditing, or feasibility and scope assessment.

Conditions for failure of large IT projects have long been identified, but they remain notoriously difficult to avoid in practice due to entrenched cultural issues and the counterintuitive requirements in some areas. The failure criteria include unclear success criteria, unclear motivations, changing goals, lack of control over scope creep, designs driven by other than risk management and user-centred design priorities, testing not tied to clearly understood goals, and deferring the hardest problems (including being able to articulate what exactly the end-users want, or will at least accept) while flagging as progress easy ones (McConnell 1995).

COMPLEX PROCESS WITH OBSCURE MOTIVATION

The potential scope of a filter is very large at the upper bound: to match every transaction initiated by every click from every person using a wide array of Internet protocols against at least two lists of arbitrary size and, in the case of the proposed second tier, dynamic content.

There is a repeated history of failure in massive IT systems with uncertain or sectional popular buy-in, limited transparency, hobbled governance, shifting goals and scope, and limited connection with the actual wants and needs of the user base. While there is certainly scope for useful voluntary application of filtering in limited circumstances (whether at PC, browser or ISP level), an Internet-wide mandatory application of ISP-level filtering of Australian-defined 'potentially prohibited content' is no more than an exercise in heroic aspiration.

DOES IT MATTER IF THE MANDATORY FILTER FACES AN IMPOSSIBLE CHALLENGE?

Perversely, the abiding benefit of implementing a system that is doomed to failure (if we assume, as some supporters might, that the target is to filter the original broad class that matches the criteria for 'potentially prohibited' content) is the unmatched opportunity it presents to demonstrate strength of moral and political character. Where legislators perceive failures as being mere setbacks – small flaws capable of remedy by redoubled effort – an impossible challenge may, perversely, become a moral imperative, and 'we just need to try harder' the motto.

The natural result can be an escalating series of attempts, each time expanding in scope, not to mention cost. There is, accordingly, a real risk that policy makers would employ the predictable failure of the ISP filtering system as a justification to do more of the same so as to prove one's moral strength, rather than accept it as cause for rational reconsideration and reassessment of design or goals.

'THE GIFT THAT KEEPS ON GIVING'

Consequently, attempting an impossible challenge can, in the absence of rigorous feedback, keep providing justifications to continue in the face of highly likely failure.

Because the range of communication and encryption methods is very broad and continually growing, and increasing numbers (though still a clear minority) of Internet users are not willing to be subject to total surveillance, an Australian internet filter cannot possibly be 100% effective. This raises the question of whether failure matters.

DOES IT MATTER HOW WELL THE MANDATORY FILTER WORKS?

The Chinese Government's filtering and censorship model, while different in some significant respects from the Australian proposal, does not need or claim to be foolproof. This may be because its aim is less the total suppression of all specified unwanted activities than the creation of a widespread "chilling effect" based on secrecy, doubt and uncertainty about the true scope and specific targets of surveillance. In this context, self-censorship on a broad range of topics in a broad range of circumstances seems a sensible precaution (Watt and Maurushat 2009; Bambauer 2008a). The Chinese approach is thus one model of filtering and censorship that does not have to work 100% in order to achieve its ends.

Equally, the apparent Singaporean model of banning a nominal 100 or so sites to 'make a point' that certain material is not endorsed or accepted by the state, without actually attempting to dam the flood tide of unwelcome Internet content, provides another, less sinister, model for filtering systems whereby limited if realistic goals are achievable with vastly less than 100% accuracy, coverage or effectiveness.

Even so, while the specific goals of the proposed Australian system are only vaguely apparent, it seems to have quite different goals to the Chinese or Singaporean systems. Unlike the Chinese system, it is not framed as a general-purpose censorship tool with explicitly political aims (Bambauer et al. 2005), even though discussion of the politics of the actual censorship mechanism is already under some pressure[2] (Jacobs 2009b). On the other hand, unlike Singapore's apparent pragmatic acceptance of the reality of the impossibility of classifying or censoring the whole of the Internet, the Australian system is at least ambivalent about this impossible goal.

In the desire to hold out hope of a 'magic bullet' – a simple, quick and permanent fix to an unpleasant and hard challenge for parents – and with a new-found drive for muscular re-regulation being the order of the day, there seems to be a temptation among politicians to reap the political payoff of being the one to fire the shot. While there are frequent references in reports to the effect that there is no magic bullet, the ISP filter proposal seems destined to offer a hope that transcends its actual capacity, and which potentially confounds sober debate.

'EVIDENCE-BASED POLICY'

'Evidence-based policy' is a familiar mantra used by recent incoming governments in Britain and Australia, and features prominently in the ISP filtering policy promotion. It is certainly better to introduce relevant data, evidence and research into policy making than rely on discretion, tradition or rhetoric, but 'Evidence-based policy' without the attributes of true evidence-based analysis in other disciplines is potentially problematic.

In other words, the selective use of data and carefully framed questions can be used to support a pre-determined outcome, especially in the absence of clear initial hypotheses or goals, evidence open to scrutiny, multiple independent analyses and disinterested evaluation of methodology. (This is particularly the case where legislators will consider but the one 'option'.) As Banks has pointed out:

> In situations where government action seems warranted, a single option, no matter how carefully analysed, rarely provides sufficient evidence for a well-informed policy decision. The reality, however, is that much public policy and regulation are made in just that way, with evidence confined to supporting one, already preferred way forward. Hence the subversive expression, 'policy-based evidence'! (Banks 2009; Argyrous 2009).

POLITICAL, SECTIONAL INPUT AND CENSORSHIP DECISIONS?

It has become increasingly common for issues about community standards on the Internet or television to be politicised, and for frenzied controversy to dominate the debate. While public input and discussion are valuable, political and sectional groups trying to gain publicity often steal the limelight or impose their own views. This can over-rule genuine community standards. There should be a package of changes to de-sensationalise censorship debates in particular, and to give the diverse range of community standards better recognition.

As Malcolm Colless has suggested, some changes worth pursuing include to:

- reverse the trend to place bodies dealing with censorship, such as the current ACMA and OFLC under control of the executive government;
- oblige those bodies to regularly survey the community on community standards about obscenity, violence, portrayal of sex and similar issues;

- oblige them to regularly report to the public and the Parliament on community standards surveys;
- require them to consider broad community standards in priority to views of individuals and organisations when making censorship decisions (Colless 2008).

These prescriptions may be a useful guide to ways to move beyond the current somewhat ill-informed debates.

8. CONCLUSIONS ON THE BALANCE OF PROTECTIONS

One factor largely absent from the public debate to date is the fundamental attempt to extend executive power over international content by means not of law, but of technology. The Australian filtering proposals are potentially an architectural change to a system initially designed to route around blockages, damage and obstructions (that is, the Internet) to one where these block points are mandated, and compliance with traditional design goals becomes potentially subject to legal sanction (Brooks 2009).

In this respect, Lessig has famously suggested that our ‘real space constitution’ should inform the values of our cyberspace constitution, to at least ‘constrain the state in its efforts to architect cyberspace in ways that are inconsistent with those values’ (Lessig 2006). Australia enjoys no equivalent to the US *Constitution’s* First Amendment in support of freedom of speech, which has seen off past legislative attempts to render the whole (American) Internet ‘safe for children’ (AFP 2009). In this context, the combination of rapidly expanding legal ‘potential prohibition’ of content outside Australian jurisdiction, and the proposal to implement filtering in hardware and software rules, should be cause for concern.

In coming to a conclusion, it is important to acknowledge the fears and concerns of many parents faced with the sometimes intractable issues arising from their children's’ use of modern communications technologies, which are increasingly convergent and rich. However, while some acknowledgement is offered in policy circles that there is ‘no silver bullet’, it appears that the ISP filtering proposal does often seem like a seductive panacea for both parent and politician alike, while offering limited practical capacity in reality, and perhaps distracting attention from the more prosaic but effective human mechanisms for building that sceptical resilience amongst young people which can help inoculate them against the wider array of real online risks.

It will take careful unravelling of the real options, risks and limitations of various technical mechanisms to engage both unruly groups in serious debate about the most effective way to characterise and to promote the interests of young people online.

Meanwhile, what we have looks like an expensive technical solution to the doomed challenge of making the whole online world 'safe for children', a cause already rejected in the US on constitutional grounds. The Australian government’s filtering proposal is inimical to both net neutrality and traditional notions of the limits of executive government’s rights to censor and restrain free speech. It is unlikely to work in practice to effectively address either the threat of child pornography/child abuse material, or access to material with some capacity for harm. The current fascination with it may, in fact, be diverting us from the real task, which is how to listen to young people and work together with them to evolve an open and robust means for spreading the robustness and common sense they will need in the online future.

While encouraging a healthy scepticism and disrespect of authority may be one gift to young people from the current filtering melodrama, we can surely offer a more straightforward engagement with real risks and opportunities.

ACKNOWLEDGEMENTS

The authors benefited from generous assistance from colleagues and interns including Alana Maurushat, Reg Leones, Adam Arnold and Joanna Chow.

APPENDIX: NATIONAL CLASSIFICATION CODE

Federal Register of Legislative Instruments F2005L01284: http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrument1.nsf/0/A9975715C45E4DE8CA25700D002EF639/$file/Code+26+May_to+attach.pdf. (No date or revision information shown in the body of the document or attached Notes).

1. Classification decisions are to give effect, as far as possible, to the following principles:

a) adults should be able to read, hear and see what they want;

b) minors should be protected from material likely to harm or disturb them;

c) everyone should be protected from exposure to unsolicited material that they find offensive;

d) the need to take account of community concerns about:

e) depictions that condone or incite violence, particularly sexual violence; and

f) the portrayal of persons in a demeaning manner.

PUBLICATIONS

2. Publications are to be classified in accordance with Table 2:

Item	Description of publication	Classification
1	Publications that: (a) describe, depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or (b) describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not); or (c) promote, incite or instruct in matters of crime or violence	RC
2	Publications (except RC publications) that: (a) explicitly depict sexual or sexually related activity between consenting adults in a way that is likely to cause offence to a reasonable adult; or (b) depict, describe or express revolting or abhorrent phenomena in a way that is likely to cause offence to a reasonable adult and are unsuitable for a minor to see or read	2 Category 2 restricted
3	Publications (except RC publications and Category 2 restricted publications) that: (a) explicitly depict nudity, or describe or impliedly depict sexual or sexually related activity between consenting adults, in a way that is likely to cause offence to a reasonable adult; or (b) describe or express in detail violence or sexual activity between consenting adults in a way that is likely to cause offence to a reasonable adult; or (c) are unsuitable for a minor to see or read	R 18+
4	All other publications Unrestricted	MA 15+

Table 2

FILMS

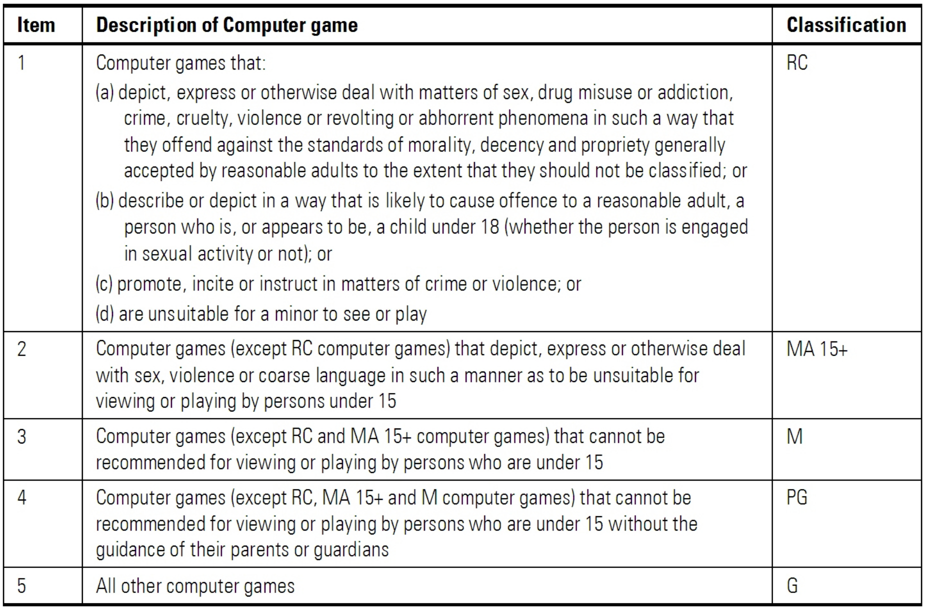
3. Films are to be classified in accordance with Table 3:

Item	Description of film	Classification
1	Films that: (a) depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or (b) describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be , a child under 18 (whether the person is engaged in sexual activity or not); or (c) promote, incite or instruct in matters of crime or violence	RC
2	Films (except RC films) that: (a) contain real depictions of actual sexual activity between consenting adults in which there is no violence, sexual violence, sexualised violence, coercion, sexually assaultive language, or fetishes or depictions which purposefully demean anyone involved in that activity for the enjoyment of viewers, in a way that is likely to cause offence to a reasonable adult; and (b) are unsuitable for a minor to see	X 18+
3	Films (except RC films and X 18+ films) that are unsuitable for a minor to see	R 18+
4	Films (except RC films, X 18+ films and R 18+ films) that depict, express or otherwise deal with sex, violence or coarse language in such a manner as to be unsuitable for viewing by persons under 15	MA 15+
5	Films (except RC films, X 18+ films, R 18+ films and MA 15+ films) that cannot be recommended for viewing by persons who are under 15	M
6	Films (except RC films, X 18+ films, R 18+ films, MA 15+ films and M films) that cannot be recommended for viewing by persons who are under 15 without the guidance of their parents or guardians	PG
7	All other films	G

Table 3

COMPUTER GAMES

4. Computer games are to be classified in accordance with Table 4:



Item	Description of Computer game	Classification
1	Computer games that: (a) depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or (b) describe or depict in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not); or (c) promote, incite or instruct in matters of crime or violence; or (d) are unsuitable for a minor to see or play	RC
2	Computer games (except RC computer games) that depict, express or otherwise deal with sex, violence or coarse language in such a manner as to be unsuitable for viewing or playing by persons under 15	MA 15+
3	Computer games (except RC and MA 15+ computer games) that cannot be recommended for viewing or playing by persons who are under 15	M
4	Computer games (except RC, MA 15+ and M computer games) that cannot be recommended for viewing or playing by persons who are under 15 without the guidance of their parents or guardians	PG
5	All other computer games	G

Table 4

ENDNOTES

[1] As we write, there have emerged unconfirmed suggestions for the first time that there may be some external oversight of the ACMA list, perhaps by ‘eminent Australians’ (Harrison 2009). Why operation and oversight of a list of prohibited material list should not primarily be the domain of the Classification Board is unclear, although the recent diminution of its independence may have undermined confidence that it can perform its traditional role.

Equally significant for the oversight of the black list is the sheer resources that would be required to properly assess and classify even a minute proportion of the Web and other online content sources, if the list were to include most items that met its inclusion Classification criteria.

While moves towards transparency would be welcome, neither of these problems are obviously solved by enlisting ‘eminent Australians’, who may or may not be more prone to political selection than the professional Classification Board or ACMA staff.

[2] For instance, the EFA and Whirlpool link deletion takedown notices, which ironically themselves either must be suppressed or undermine their own effect: they must include the very URL whose suppression they intend, so publication of them would undermine their operation (Jacobs 2009a).

REFERENCES

AAP 2009. ‘Web blacklist won’t stop child porn, admits Communications Minister Senator Conroy’, *News* online, 30 March 2009, http://www.news.com.au/technology/story/0,28348,25262960-5014239,00.html.

ABC 2009. 'Qld police help bust global child porn ring', ABC online news, 16 January 2009, http://www.abc.net.au/news/stories/2009/01/17/2468237.htm.

ACMA 2009a. 'Developments in internet filtering technologies and other measures for promoting online safety – Second Annual Report to the Minister for DBCDE.' April (date on title page and apparent publication date) or 2008 (copyright notice date), http://www.acma.gov.au/webwr/_assets/main/lib310554/developments_in_internet_filters_2ndreport.pdf and http://www.acma.gov.au/WEB/STANDARD/pc=PC_311304.

ACMA 2009b. 'ACMA list of prohibited and potentially prohibited overseas hosted content.' 19 March, http://acma.gov.au/WEB/STANDARD/pc=PC_311669.

ACMA 2009c. Australia in the Digital Economy: Report 1 – Trust and Confidence, Australia in the Digital Economy research report series, March, http://www.acma.gov.au/webwr/aba/about/recruitment/trust_and_confidence_aust_in_digital_economy.pdf.

ACMA 2008a. 'Complaint from the public results in network of child sexual abuse websites being brought down.' ACMA media release 118/2008, 1 October, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311406.

ACMA 2008b. Closed environment testing of ISP-level Internet content filtering – a report. July, http://www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf.

ACMA 2008c. 'ACMA approves industry code of practice to protect children from unsuitable online and mobile phone content here.' ACMA media release 88/2008, 16 July, http://www.acma.gov.au/WEB/STANDARD/912091/pc=PC_311247.

ACMA 2008d. Annual Report 2007–08. <http://www.acma.gov.au/WEB/STANDARD/pc=PC_100770> Table 25, 'Prohibited/potentially prohibited Internet content 2007–08, items actioned', Chapter 2: Regulatory environment (continued) - Compliance investigations, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311421 - compliance.

ACMA 2008e. 'Community awareness' page. (elsewhere linked as 'national cybersafety education program'), undated, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90161.

ACMA 2008f. 'Online content complaints.' Fact Sheet FS 122, January, http://www.acma.gov.au/WEB/STANDARD/pc=PC_310727.

ACMA n.d.a. 'Internet service providers and law enforcement and national security.' Fact Sheet, undated, http://www.acma.gov.au/WEB/STANDARD/pc=PC_100072.

ACMA n.d.b. 'Internet service providers interception obligations', Fact Sheet, undated, http://www.acma.gov.au/WEB/STANDARD/pc=PC_100073.

ACMA n.d.c. 'Prohibited Online Content', undated, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102.

ACMA 2007. Developments in internet filtering technologies and other measures for promoting online safety, First annual report to the Minister for BCDE, February 2008 (copyright 2007), http://www.acma.gov.au/webwr/_assets/main/lib310554/developments_in_internet_filters_1streport.pdf.

ACMA 2006. ISP code compliance audit: Audit of ISP compliance with the consumer protection obligations under the internet content codes of practice,’ April 2006, http://www.acma.gov.au/webwr/aba/contentreg/codes/internet/documents/isp code compliance audit.pdf.

ACMA 2005. 'Online content codes', May 2005, http://www.acma.gov.au/WEB/STANDARD/pc=PC_90080.

AFP press syndicate 2009. ‘US Supreme Court shuts door on *Child Online Protection Act’*. ABC News Online. 22 Jan 2009, http://www.abc.net.au/news/stories/2009/01/22/2472227.htm.

Albury, Kath; Lumby, Catharine and McKee, Alan. 2008. 'The Pursuit of Innocents.' New Matilda, 6 June, http://newmatilda.com/2008/06/06/pursuit-innocents.

Alpert, Jesse; Hajaj, Nissan. 2008. ‘We knew the web was big…’ Official Google blog, 25 July 2008, http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html.

Anderson 2007. ‘Deep Packet Inspect Meets Net Neutrality, CALEA’, 25 July 2007, *Ars Technica*, http://arstechnica.com/hardware/news/2007/07/Deep-packet-inspection-meets-net-neutrality.ars, at 23 May 2009.

Annetta 2008. 'First They Came For The Perverts.' New Matilda, 23 Oct 2008, http://newmatilda.com/2008/10/23/first-they-came-perverts.

Argyrous 2009. *Evidence for Policy and Decision-Making: A Practical Guide*. Sydney: UNSW Press.

Australian Government 2008. NetAlert. FAQ (free PC filters not available past 31 Dec 2008), http://www.netalert.gov.au/filters/faqs.html - q15.

ATMA v Cth 1993. *Australian Tape Manufacturers Association Ltd v Commonwealth (‘ATMA v Cth’)* (1993) 176 CLR 480.

Bambauer 2008a. 'Guiding the Censor's Scissors: Assessing Internet Filtering', Brooklyn Law School Legal Studies Research Papers Working Paper Series, 10 June 2008. SSRN, http://ssrn.com/abstract=1143582.

Bambauer 2008b. 'Filtering in Oz: Australia's Foray Into Internet Censorship'. Brooklyn Law School Legal Studies Research Papers Working Paper Series, Research Paper No. 125, December 2008 SSRN, http://ssrn.com/abstract=1319466.

Bambauer, Derek. Ronald Deibert. John Palfrey, Rafal Rohozinski, Nart Villeneuve, Jonathan Zittrain. 2005. 'Internet Filtering in China in 2004-2005: A Country Study.’ Berkman Center for Internet & Society at Harvard Law School, Research Publication No. 2005-10, 15 April 2005, SSRN, http://ssrn.com/abstract=706681.

Banks, Gary (Chairman, Productivity Commission).2009. ‘Evidence-based policy-making: What is it? How do we get it?’ ANZ School of Government/ANU Public Lecture Series 2009. Canberra, 4 February, p.8, http://www.pc.gov.au/__data/assets/pdf_file/0003/85836/cs20090204.pdf.

Bermeister, Kevin (Brilliant Digital Entertainment). 2009. Presentation at the second Cyberspace Law and Policy Centre Internet filtering and censorship proposals forum, Baker & McKenzie Sydney office, 10 March 2009.

Beveridge, Sue. 2009. (NSW Department of Education and Training, NSW Connected Classrooms program). 2009. ‘NSW Education Department filtering.’ Presentation for the Internet society forum ‘Unacceptable’ Content On The Internet: What Problem? Whose Solution?.’ Sydney: Google Offices, 18 May 2009.

Bingemann, Mitchell. 2009. 'Filter plan angers Labor youth base.' *The Australian IT*, 2 June 2009, http://www.australianit.news.com.au/story/0,,25571450-5013040,00.html.

Bradley, Caroline. Froomkin, Michael. 2006. ‘Virtual Worlds, Real Rules: Virtual worlds to test legal rules.’ In Balkin, Jack and Noveck, Beth Simone, *State of Play: Law Games and Virtual Worlds*, New York: New York University Press.

Brockie, Jenny (presenter).2009. ‘Blocking the net – will it make kids any safer?’ *Insight* transcript. SBS Television, 7:30 PM. 31 March, http://news.sbs.com.au/insight/episode/index/id/59 - watchonline.

Brooks, Paul (ISOC-AU). 2008. ‘Internet Filtering: What it is – and isn’t…’. presentation for the first Cyberspace Law and Policy Centre Internet filtering and censorship proposals forum. UNSW Law Faculty. Sydney, 27 November, http://cyberlawcentre.org/2008/censorship/Content_Filtering-Paul Brooks-ISOC_format.pdf.

Brooks, Paul (ISOC-AU). 2009. ‘Internet Filtering: What it is – and What it still isn’t…’. Presentation for the second Cyberspace Law and Policy Centre Internet filtering and censorship proposals forum, Baker & McKenzie, Sydney, 10 March 2009, http://cyberlawcentre.org/censorship/presentations/3_Brooks.pdf.

Broadcasting Services Act 1992 (Cth) (‘BSA’), http://www.austlii.edu.au/au/legis/cth/consol_act/bsa1992214 Schedule 5 Online services, Schedule 7 Content services, ACMA role.

Carlisle, Wendy (producer). 2009. 'Conroy's clean feed.' ABC Radio National, Background Briefing transcript, 15 March, http://www.abc.net.au/rn/backgroundbriefing/stories/2009/2512171.htm and MP3 audio: http://mpegmedia.abc.net.au/rn/podcast/2009/03/bbg_20090315.mp3.

Classification Policy Branch 2006. *National classification scheme*. Attorney-Generals Department (Cth), created 6 September 2006, modified 25 March 2009, http://www.ag.gov.au/www/agd/agd.nsf/Page/Classificationpolicy_Nationalclassificationscheme.

Classification Policy Branch, n.d. *Classification Research*. Attorney-Generals Department (Cth) (not dated), http://www.ag.gov.au/www/agd/agd.nsf/Page/Classificationpolicy_Research.

Classification (Publications, Films and Computer Games) Act 1995 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/cfacga1995489/.

Classification (Publications, Films and Computer Games) Regulations 2005 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_reg/cfacgr2005598/.

Colless, Malcolm. 2008 ‘Content of communications’. Interview, *Network Insight*. July, http://www.networkinsight.org/4_content_of_communications.html.

Colley, Andrew. 2009. ‘Net filtering may not be mandatory.’ *The Australian IT*, 26 May, http://www.australianit.news.com.au/story/0,24897,25542310-15306,00.html.

Collins, Louise; Love, Peter; Landfeldt, Dr Bjorn; Coroneos, Peter. 2008. 'Feasibility Study - ISP Level Content Filtering February.' Report to DBCDE submitted 2008, released January 2009, http://www.dbcde.gov.au/__data/assets/pdf_file/0006/95307/Main_Report_-_Final.pdf.

Communications Legislation Amendment (Content Services) Act 2007 (Cth), http://www.austlii.edu.au/au/legis/cth/num_act/clasa2007544/.

Communications Legislation Amendment Act (No. 1) 2003 (Cth). Schedule 2: Freedom of Information Act 1982, http://www.austlii.edu.au/au/legis/cth/num_act/claa12003395/sch2.html.

Conroy, Senator Stephen. 2009. 'Optus to participate in ISP filtering pilot.’ Media release, 22 April, http://www.minister.dbcde.gov.au/media/media_releases/2009/027.

Conroy, Senator Stephen. 2007. *Labor's Plan for Cyber Safety*. Australian Labor Party, Election 07 Fact Sheet. (undated – November 2007?), http://www.alp.org.au/download/now/labors_plan_for_cyber_safety.pdf.

Coonan, Helen (former Minister). 2007a. Protecting Australian Families Online Direction No. 1 of 2007. Ministerial direction to ACMA. 9 Jun 2007, http://www.acma.gov.au/webwr/_assets/main/lib310032/dir_1of07_protect_aust_families_online.pdf [Instructions to conduct filtering trial, purposes etc.].

Coonan, Helen (former Minister). 2007b. Protecting Australian Families Online Direction No. 2 of 2007. Ministerial direction to ACMA. 9 Jun 2007, http://www.acma.gov.au/webwr/_assets/main/lib310032/dir_2of07_protect_aust_families_online.pdf [Instructions to report by 31 December each year on developments in filtering.].

Copyright Act 1968 (Cth) ss 31(1)(a)(iv), 85(1)(a), 85(1)(c), 86(a) & (c), 87(a) & (c), 89, 90, 91, 196, http://www.austlii.edu.au/au/legis/cth/consol_act/ca1968133/.

Criminal Code 1995 (Cth), s474.19 'Using a carriage service for child pornography material', s474.23 'Using a carriage service for child abuse material', http://www.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html.

Criminal Code 1999 (Qld), s228C 'Distributing child exploitation material', http://www.austlii.edu.au/au/legis/qld/consol_act/cc189994/s228c.html.

Crimes Act 1900 (NSW), s91H 'Production, dissemination or possession of child pornography', http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/s91h.html.

DBCDE. 2008a. 'Technical Testing Framework, ISP Filtering Live Pilot.’11 November 2008, http://www.dbcde.gov.au/__data/assets/pdf_file/0006/89160/technical-testing-framework.pdf.

DBCDE. 2008b. 'ISP Filtering Live Pilot - Questions and answers', undated [Nov 2008?], http://www.dbcde.gov.au/communications_for_business/funding_programs__and__support/isp_filtering_live_pilot/questions_and_answers.

DBCDE. 2008c. 'Internet Service Provider (ISP) Content Filtering 'Live' Pilot.' undated [11 November 2008?], http://www.dbcde.gov.au/communications_for_business/funding_programs__and__support/isp_filtering_live_pilot.

DBCDE. 2008d. 'Request for Expression of Interest.' ISP Filtering Live Pilot, 11 November 2008, http://www.dbcde.gov.au/__data/assets/pdf_file/0005/89159/request-for-expression-of-interest.pdf.

Doel-Mackaway, Holly (child rights advisor, Save the Children Australia) and McDougall, James (director, National Childrens and Youth Law Centre). 2008. 'A Child Rights Perspective on the Federal Government's Internet Filtering Proposal.' Presentation for the first Cyberspace Law and Policy Centre Internet filtering and censorship proposals forum. UNSW Law Faculty. Sydney, 27 November at: http://cyberlawcentre.org/2008/censorship/Presentations/31_Holly.pdf.

EU. 2007. 'Telecoms Package' COD/2007/0247 and COD/2007/0248.

Flood, Michael; Hamilton, Clive. 2003. Regulating Youth Access to Pornography. Discussion Paper Number 53, The Australia Institute, March, https://www.tai.org.au/file.php?file=DP53.pdf.

Graham, Kerry. (Inspire Foundation). 2009. 'Measures to keep children and young people safe online.' Presentation for the second Cyberspace Law and Policy Centre Internet filtering and censorship proposals forum. Sydney: Baker & McKenzie. 10 March.

Graham, Irene. 2000. 'Is the OFLC dysfunctional?' Libertus.net, *Australia's censorship system*, http://libertus.net/censor/rdocs/oflc2structure.html.

Griffith, Gareth. 2009. 'Censorship law - questions and answers.' E-BRIEF No. 5/2009, NSW Parliamentary Library Research Service, May, http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/7230302B 505A9D4FCA2575AF007F7462/$File/E Brief Censorship law - questions and answers.pdf.

Griffith, Gareth, and Simon, K. 2008. Child Pornography Law. Briefing Paper No 9/08, NSW Parliamentary Library Research Service, August, http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/289C584B 88554BCBCA2574B400125787/$File/Child pornography law and index.pdf.

Ghosh, Ajoy (digital forensics expert, Logica). 2008. 'Lessons from prosecutions of Child Pornography and other "prohibited" material.' Presentation for the first Cyberspace Law and Policy Centre Internet filtering and censorship proposals forum, UNSW Law Faculty, Sydney, 27 November, http://cyberlawcentre.org/2008/censorship/Presentations/32_Ajoy Ghosh.pdf.

Guidelines for the Classification of Films and Computer Games 2005 (Cth), http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200508205.

Guidelines for the Classification of Publications 26 May 2005, approved by Commonwealth, State and Territory Censorship Ministers, http://www.comlaw.gov.au/comlaw/Legislation/LegislativeInstrument1.nsf/0/E03BF15D1B 9B9CDCCA25700D00284712.

Hansard 2008a. Senate Estimates Environment, Communications, and the Arts Committee, 20 October 2008, p.78 and following, Senators Ludlam and Conroy, http://www.aph.gov.au/hansard/senate/commttee/S11346.pdf.

Hansard 2008b. Senate debates, 3 December 2008, p.8013, 'Questions without Notice: Internet Filtering', Senators Conroy and Bernardi, questions re filter trial, http://www.aph.gov.au/hansard/senate/dailys/ds031208.pdf Video: http://www.youtube.com/watch?v=9XnZPtt-PMs.

Hansard 2009a. Senate Estimates, Environment, Communications, and the Arts Committee, 23 February 2009, Senators Conroy, Bernardi and others, at: http://www.aph.gov.au/hansard/senate/commttee/S11635.pdf.

Hansard 2009b. Senate Estimates, Environment, Communications, and the Arts Committee, 25 May 2009, Senators Conroy, Bernardi. Ludlam, Minchin and others, from ECA 99, http://www.aph.gov.au/hansard/senate/commttee/S12031.pdf.

Hanmore, Karl (AusCERT). 2009. presentation at the second Internet filtering and censorship proposals forum, Baker & McKenzie, Sydney, 10 March.

Harrison, Dan. 2009. 'Review of website blacklist in wind.' The Age (Mebourne), 27 May, http://www.theage.com.au/national/review-of-website-blacklist-in-wind-20090526-bm4s.html.

Horten, Monica. 2009. ‘How the EU Is Bargaining Away the Internet’, http://www.iptegrity.com/index.php?option=com_content&task=view&id=287&Itemid=9, 23 May.

Internet Industry Association (IIA). 2008. ‘Internet Industry Code of Practice: *Content Services Code* for Industry Co-Regulation in the Area Of Content Services (Pursuant to the Requirements of Schedule 7 of the Broadcasting Services Act 1992 as amended).’ (‘*Content Services Code*’), 24 June, current as of May 2009, http://www.acma.gov.au/webwr/_assets/main/lib310679/registration_of_content_svces_code.pdf. See also:
http://www.iia.net.au/images/content_services_code_registration_version_1.0.pdf.

IIA. 2006. *Mandatory Server Level Filtering*. Position Statement, 11 April, http://www.iia.net.au/index.php/component/content/462.html?task=view. See also similar statement of 28 August 2007, http://www.iia.net.au/index.php/component/content/article/49/587-mandatory- server-level-filtering.html and 20 March 2006, http://www.iia.net.au/index.php/component/content/article/1/450-iia-questions-alp-policy-on-internet-filtering.html.

IIA. 2005. *Internet Industry Codes of Practice Codes For Industry Co-Regulation In Areas Of Internet And Mobile Content (Pursuant To The Requirements Of The Broadcasting Services Act 1992)* May (Includes Provisions Affecting Mobile Services) Version 10.4 . Current as of May 2009, http://www.acma.gov.au/webwr/aba/contentreg/codes/internet/documents/iia_code_2005.pdf.

Internet Watch Foundation. 2008. Annual Report 2007. April 2008, http://www.iwf.org.uk/documents/20080417_iwf_annual_report_2007_(web).pdf ['UK Hotline for reporting illegal content, specifically, child sexual abuse content hosted worldwide, and criminally obscene and incitement to racial hatred content hosted in the UK'].

Jacobs, Colin. 2009a. 2009. ‘EFA gets link removal notice.’ Electronic Frontiers Australia (EFA). 5 May, http://www.efa.org.au/2009/05/05/efa-gets-link-removal-notice/.

Jacobs, Colin. 2009b. ‘Net censorship already having a chilling effect.’ Electronic Frontiers Australia (EFA). 13 March, http://www.efa.org.au/2009/03/13/net-censorship-already-having-a-chilling-effect/.

Kravets, David. 2009. 'WikiLeaks Exposes Australian Web Blacklist.' Wired, 19 March, http://blog.wired.com/27bstroke6/2009/03/wikileaks-expos.html.

Lessig, Lawrence. 2006. *Code 2.0* (version 2.0 of *Code and Other Laws of Cyberspace*). New York: Basic Books.

Lindsay, David; Sharon Rodrick; Melissa de Zwart. 2008. ‘Regulating Internet and convergent mobile content’. *Telecommunications Journal of Australia*. November 2008. Vol. 58, No. 2-3. p.31-1. DOI: 10.2104/tja09031, http://publications.epress.monash.edu/doi/full/10.2104/tja08031.

Maher, Rachel. 2009. 'The More Untangled the Web Becomes…' New Matilda, report of New Matilda forum in Sydney, 8 May, http://newmatilda.com/polliegraph/?p=636.

Malamuth, Neil; Huppin, Mark. 2005. ‘Pornography and Teenagers: The Importance of Individual Differences.’ *Adolesc Med* 16 315–326; cited by Carlisle 2009, above.

McConnell, Stephen. 1995. *Rapid Application Development*. Microsoft Press.

McDougall, James (director, National Childrens and Youth Law Centre). 2009 ‘Using a Child Rights Framework’, presentation for the second Cyberspace Law and Policy Centre Internet filtering and censorship proposals forum. Baker & McKenzie. Sydney, 10 March, http://cyberlawcentre.org/censorship/presentations/1 McDougall.pdf.

McEwen v Simmons & anor [2008] NSWSC 1292 (8 December), NSW Supreme Court, Judge Adams J., http://www.austlii.edu.au/au/cases/nsw/supreme_ct/2008/1292.html.

Moses, Asher. 2009. 'Blacklist snares Bill Henson fan site,' *SMH online*, 26 March 2009, http://www.smh.com.au/articles/2009/03/26/1237657050527.html.

Moses, Asher. 2009. ‘Christians upset at Conroy's net policy “backtrack”’. The *Age*, 27 May, http://www.theage.com.au/articles/2009/05/27/1243103585180.html.

Moses, Asher. 2008a. 'Wikipedia added to child pornography blacklist,' SMH online, 8 December, http://www.smh.com.au/articles/2008/12/08/1228584723764.html.

National Classification Code. n.d. Federal Register of Legislative Instruments F2005L01284, http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrument1.nsf/0/A9975715C45E4DE8CA25700D002EF639/$file/Code+26+May_to+attach.pdf.

Newton, Mark. 2009. 'Senator Conroy Blacklists His Own Police', New Matilda, 14 April, http://newmatilda.com/polliegraph/?p=567.

O'Toole, Kate (interviewer). 2009. *Hack* interview audio. ABC Radio Triple-J. 7 April, http://mpegmedia.abc.net.au/triplej/hack/daily/hack_tues_2009_04_07.mp3.

Office of the Privacy Commissioner of Canada. 2009. Deep Packet Inspection: A Collection of Essays from Industry Experts. OPCC website, http://dpi.priv.gc.ca/.

Ohm, Paul. 2008. 'The Rise and Fall of Invasive ISP Surveillance.' *University of Colorado Law School Legal Studies Research Series*, Working Paper 08–22.

Parsons, Christopher. 2008. 'Deep Packet Inspection in Perspective: Tracing Its Lineage and Surveillance Potentials.' *The New Transparency: Surveillance and Social Sorting*, Working Paper.

Privacy Act 1988 (Cth), s 6, Sch 3 cl 1.1., http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/.

Seven Network (Operations) Limited v Media Entertainment and Arts Alliance ('Seven v MEAA') [2004] FCA 637, http://www.austlii.edu.au/au/cases/cth/FCA/2004/637.html.

SMH Online editors, individual contributors. 2006. 'What are your memories of Don Chipp?' *SMH* Newsblog, 29 August, http://blogs.smh.com.au/newsblog/archives/your_say/005697.html?page=fullpage - comments.

Tenants' Union of Queensland Inc, Tenants' Union of NSW Co-op Ltd v TICA Default Tenancy Control Pty Ltd ('*Tenants' Union*') [2004] PrivCmrACD 4, http://www.austlii.edu.au/au/cases/cth/PrivCmrACD/2004/4.html.

Universal Music Australia Pty Ltd v Sharman License Holdings Ltd ('*Sharman*') [2005] FCA 1242, http://www.austlii.edu.au/au/cases/cth/FCA/2005/1242.html.

Vaile, David. 2009. *Internet filtering and young people references*. Sydney: Cyberspace Law and Policy Centre, http://cyberlawcentre.org/censorship/references.htm.

Wallace, Jim (Australian Christian Lobby). 2009. 'Filtering filth will not tangle the net.' Opinion piece, *SMH* online, 26 January, http://www.smh.com.au/news/opinion/filtering-filth-will-not-tangle-the-net/2009/01/ 25/1232818241442.html.

Watt, Renée; Maurushat, Alana. 2009. "Clean Feed: Australia's Internet Filtering Proposal" [2009] UNSWLRS 7; also *Internet Law Bulletin* March, http://www.austlii.edu.au/au/journals/UNSWLRS/2009/7.html.

Working Group against Internet blocking and censorship (AK Zensur). 2009. 'Delete, don't block: It works! Within 12 hours, 60 child pornography sites were removed from the internet' Media release (English translation from the German). 28 May, http://www.unpolitik.de/2009/05/28/delete-dont-block-it-works/ and http://ak-zensur.de/.

Wu, Tim. 1999. 'Internet v Application: Application-Centered Internet Analysis', Working Paper Series, 15 March 15, SSRN, http://ssrn.com/abstract=157928.

X (anonymous source). 2009. 'An insight into child porn: 10 years inside the international child porn industry with our confidential source.' Wikileaks, 26 February, https://secure.wikileaks.org/wiki/An_insight_into_child_porn.

Yu, Peter. 2008. 'The Escalating Copyright Wars'. *HOFSTRA Law Review*, 32, 907.

Cite this article as: Vaile, David; Watt, Reneé. 'Inspecting the despicable, assessing the unacceptable: Prohibitied packets and the great firewall of Canberra'. *Telecommunications Journal of Australia*. 59 (2): pp. 27.1 to 27.35. DOI: 10.2104/tja09027.