PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES

PARLIAMENTARY LIBRARY
INFORMATION ANALYSIS ADVICE
RESEARCH PAPER

RESEARCH PAPER SERIES, 2014–15 8 AUGUST 2014

Australian Governments and dilemmas in filtering the Internet: juggling freedoms against potential for harm

Paula Pyburne, Law and Bills Digest
Dr Rhonda Jolly, Social Policy

Executive summary

- The Internet is a revolutionary source of information and its dissemination; and a medium for collaboration and interaction between individuals without regard for geographic location.
- Since its inception, however, concerns have been raised about the potential for unsavoury characters to use the Internet as a vehicle for distributing pornography and material of a violent nature to young or otherwise vulnerable individuals.
- Governments across the world have attempted to deal with such activities by various means and to varying degrees. These have included imposing mandatory filtering at an Internet Service Provider (ISP) level and optional filtering at the computer level.
- In Australia there has been considerable debate about what degree of filtering (if any) should be mandated.
- The Howard Government favoured an approach which emphasised self-regulation by ISPs combined with a legislative component and education and freedom for families to choose between either computer or ISP filtering based on a list of unacceptable content.
- The Rudd and Gillard Governments preferred the option of a mandatory ISP level filter, although this too was to be based on a 'blacklist' of prohibited content.
- Both options have been criticised as being expensive and inefficient. In addition, it has been argued that the Rudd/Gillard option would have had a detrimental impact on Internet speeds and that it would set a precedent for future governments to widen filtering to other forms of expression.
- The Howard Government's programs were largely discarded by Labor after it was elected in 2007. However, Labor's own filtering option was abandoned prior to its defeat in the 2013 election.
- In conjunction with their filtering options, both Coalition and Labor Governments have supported education and information campaigns to assist people, particularly children, to deal with online predators and both have introduced successful programs.
- The current Coalition Government's policy on Internet filtering appears to favour light-handed legislation combined with education and information programs. This paper examines the iterations of internet filtering policies from the 1990s to 2014 and discusses some of their ideological underpinnings.

ISSN 2203-5249

Contents

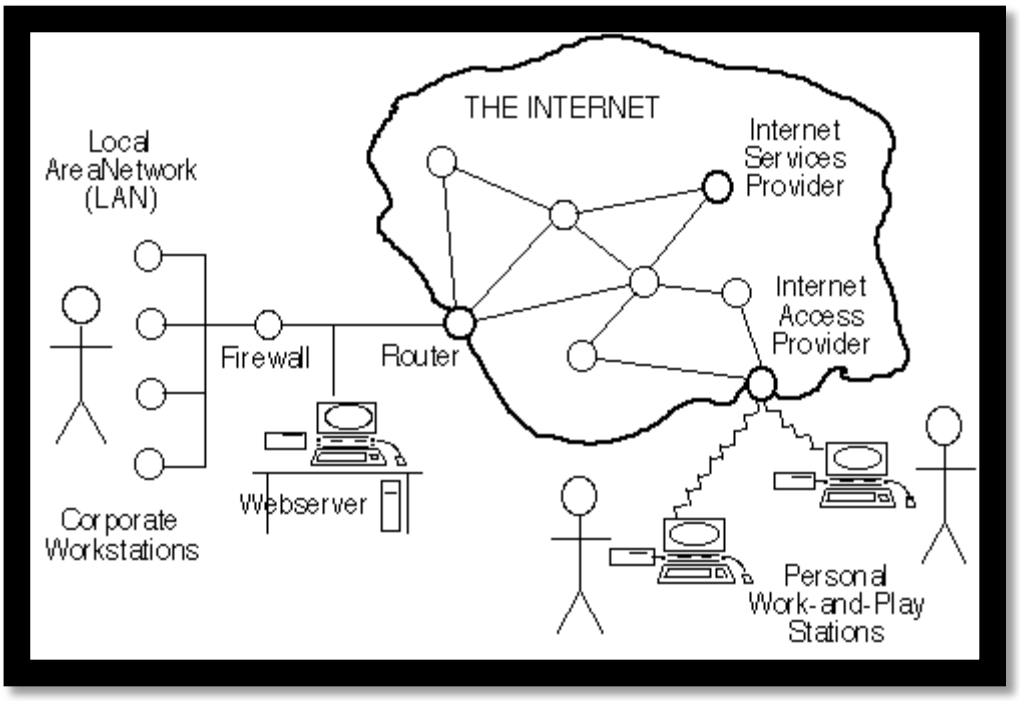
Introduction

The Internet (or Net) is the global digital infrastructure that connects millions of computers across the world, through public telephone and communication networks.[1] (The image in Figure 1 provides a simple explanation of how this occurs.)

The Net has revolutionised communications by introducing at once a world-wide broadcasting capability, a mechanism for information dissemination and a medium for collaboration and interaction between individuals via personal computers without regard for geographic location.[2]

But the geographic reach of the Internet and the anonymity it ostensibly provides has attracted a variety of unsavoury characters. It is a tool used by identity thieves, financial fraudsters and child pornographers—to name a few.

Figure 1: the Internet as perceived by users



Source: Clarke[3]

The view expressed by one multi-national company specialising in internet services, Google, is that the Internet:

> … was built and has thrived as an open platform, where individuals and entrepreneurs can connect and interact, choose marketplace winners and losers, and create new services and content on a level playing field. This openness helps spark new ideas, innovation and economic growth. Openness also enables the proliferation of diverse voices on the web.[4]

This is the fundamental premise on which the Internet was built and upon which it was intended to function—openness and freedom to connect to, and interact with other users. In the view of one modern political philosopher, some of the creators of the Internet believed that it would form the basis of a utopian social

1. The Internet uses the Internet Protocol as the principal communications protocol for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.
2. B Leiner, V Cerf, D Clark, R Kahn, L Kleinrock, D Lynch, J Postel, L Roberts and S Wolff'Brief history of the Internet', Internet Society website, accessed 26 September 2013.
3. R Clarke, 'Origins and nature of the Internet in Australia', Roger Clarke's website, 29 January 2004, accessed 7 April 2014.
4. Google, 'Open Internet and broadband access page', Google website, accessed 14 November 2013.

society.[5] Furthermore, for some of the first users of the Internet, it was seen as 'a state of perfect freedom' and a state of [information] equality, such as that described by John Locke in his treatise on the state of nature.[6]

Most people do not dispute that the Internet should be free and open to all, so that all can explore ideas and communicate across distance and cultures. At the same time, there are few who would advocate that the Internet should be a place of perfect freedom; a place where criminals should be free to exploit citizens. Most consider, as Locke did, that there is a role for government in protecting the natural rights of citizens; in the case of the Internet, in combating internet criminals and protecting vulnerable citizens from undesirable online contacts.

For these reasons the Internet has posed a number of challenges for democratic governments. These essentially are:

- to what extent should governments actively seek to regulate access to particular types of information on the Internet
- which groups should be classed as 'vulnerable' and the subject of government concern with regards to regulation and
- what should be defined as 'undesirable content' and what constitutes 'undesirable contact'.

These challenges have raised questions which have been the subject of heated debate in Australia.

As this paper illustrates, recent Australian governments have agreed that they have a role in regulating the Internet. What they have not agreed upon is the extent to which that role overrides individual choice. Disagreement on this founding premise has meant that different governments have taken different stances on the issues of what is inappropriate Internet content and what constitutes an appropriate response to filtering out undesirable elements of that content. This paper charts the evolution and frustrations involved with implementing policies which have emphasised individual choice and those which have involved what some could label a more interventionist approach.

The paper is neither intended as a detailed history of the development of the Internet or the World Wide Web, either internationally or in Australia. The paper does, however, provide a brief background of how information accessibility moved from being the property of elites into the possession of ordinary people. It does so in the context that the Internet was conceived with the idea of freedom of access and use and it was propagated with those ideas as fundamental to its development. This perception has presented governments with dilemmas regarding the extent to which the Internet can, and should be regulated.

The censorship context

From 1901, the trade and commerce power in the *Australian Constitution* enabled the Commonwealth to censor imported publications—to prohibit 'blasphemous, indecent or obscene works or articles' from entering the country.[7] Australian-produced publications, however, were regulated by state legislation.

Censorship of films in Australia began in 1917. Customs regulations prohibited the import of films that were not first approved by a Commonwealth Board of Censors. The Board of Censors was authorised to ban any film that was considered:

- blasphemous, indecent or obscene
- likely to be injurious to morality, or to encourage or incite persons to commit crime
- likely to be offensive to any ally of Great Britain or
- depicted any matter the exhibition of which, in the opinion of the Board, was undesirable in the public interest.[8]

5. PJ Burns, 'The global Internet: Utopia, democracy and the digital divide', paper presented to the annual meeting of the American Sociological Association, Montreal, 11 August 2006.
6. J Locke, *The second treatise of civil government*',1690. Locke notes: 'The natural liberty of man is to be free from any superior power on earth, and not to be under the will or legislative authority of man, but to have only the law of nature for his rule'. He continues: 'Men being, as has been said, by nature, all free, equal, and independent, no one can be put out of this estate, and subjected to the political power of another, without his own consent'.
7. *Commonwealth of Australia Constitution Act*, section 51(i), accessed 11 July 2014.

This censorship regime was both strict and complex, and it remained in place until the 1960s. As the Member for Oxley, Bill Hayden, noted in 1970 in relation to Queensland, the regime involved:

> … the Department of Customs and Excise, the Post Office, the Australian Broadcasting Control Board, the National Literature Board of Review, the Film Censorship Board, the State Literature Review Board and the State police. There are 7 bodies in all. On top of these, of course, we have in the final result the State Government and the Federal Government, if they want to effect some sort of influence on these matters. But just imagine the confusion, the conflict and the duplication that arises from the proliferation of these bodies.[9]

Beginning in the late 1960s, the censorship laws which 'rested on concepts of obscenity and indecency' were gradually replaced with a regime under which materials were classified as appropriate for certain groups.[10] Many people contributed to change in the censorship regime, including the Minister for Customs and Excise in the Gorton Liberal Government, Don Chipp, who stated before the Parliament in 1970 that the existing regulations were not appropriate for a modern society.[11]

The Whitlam Government was also convinced that adults should be able to read, view and hear what they want, but at the same time, certain people should be protected from exposure to offensive materials. Under the Whitlam administration in January 1974, the Commonwealth reached agreement with all states, except Queensland, that publications should be classified by the Commonwealth under one of three categories:

- restricted, and not for sale to those under 18—that is, material that was sexually explicit, or depicted extreme violence, horror or cruelty
- for direct sale only, by mail order—that is, 'hard core' pornography and
- prohibited—that is, publications which advocated or incited to crime, violence or the use of illegal drugs.[12]

Further reforms to the censorship regime took place in the 1980s. These coincided with the introduction of video tapes and were intended to deliver greater uniformity across state and territory laws. However, as significant differences remained between the approach of the federal government and the various states and territories, the federal government directed the Australian Law Reform Commission (ALRC) to identify problems with the existing system and to develop a model for classification laws which could apply across jurisdictions.[13]

The classification scheme which eventually resulted from an intergovernmental agreement following the ALRC's advice was based on three fundamental tenets:

- adults are entitled to read, hear and see what they wish in private and in public
- people should not be exposed to unsolicited material which is offensive to them and
- children must be adequately protected from material likely to harm or disturb them.[14]

These tenets set the framework for censorship in Australia during the earliest development of the Internet. They provided context for arguments about whether access to the Internet, and all its content, should be unfettered—or whether some form of censorship should be applied by the Government to specified content so as to limit access to that content. And in addition, whether censorship should be based on criteria already in place for films and publications.

---

8. Standing Committee on Legal and Constitutional Affairs, *Review of the national classification scheme: achieving the right balance*, Senate, Canberra, 2011, chapter 2, accessed 15 October 2013.
9. B Hayden, Speech: Censorship', House of Representatives, *Debates*, 11 June 1970, , accessed 26 September 2013.
10. D Williams (Attorney-General), *From censorship to classification*, address to Murdoch University 31 October 1997, accessed 10 February 2014.
11. D Chipp,'Ministerial statement: Censorship, House of Representatives, *Debate*s, 11 June 1970, accessed 10 February 2014.
12. Further general classification reform took place in 1983–84 with the introduction of an X rating for sexually explicit videos which could not be publicly screened, Senate Standing Committee on Legal and Constitutional Affairs, *Review of the national classification scheme: achieving the right balance*, The Senate, Canberra, 2011, chapter 2, accessed 15 October 2013 . A National Classification Scheme, underpinned by the *Classification (Publications, Films and Computer Games) Act 1995*, commenced on 1 January 1996: *Classification (Publications, Films and Computer Games) Act 1995*, accessed 15 October 2013, and Australian Classification Board, 'National Classification Scheme', Australian Classification website, accessed 15 October 2013.
13. Australian Law Reform Commission (ALRC), *Censorship procedure*, ALRC report, 55, 1991, accessed 23 July 2014.
14. G Griffith, *Censorship: law and administration*, Background paper, New South Wales Parliamentary Library, Sydney, 1993, p. 7.

Origins of the digital community

Motivation

There are a number of theories about when and how the Internet began, all of which have some credence. It is likely however, that tensions between the United States of America (America/US) and the Soviet Union in the 1950s and 1960s played a significant part in its development. The launch of the artificial satellite, Sputnik, by the Soviet Union in 1957 shocked America because of the perceived technical gap which had emerged between the powers. The US set up a military agency, the Advanced Research Projects Agency (ARPA) to explore ways through which it could retaliate against the Soviets.

Research commissioned for ARPA, as well as other academic studies, led to the development of what was called a packet switching model of networking. This model enabled communications to occur between physically separate computer systems and for US systems to respond to nuclear weapons strikes.[15] In a time when computers were very expensive this linkage allowed operators access to different computers, saving them time and travel costs. (Figure 2 below shows the first ARPA network links.)

In 1962, JCR Licklider, while working with ARPA, conceived the idea of linking computers and systems away from a purely military application. Licklider envisaged 'an Intergalactic Network where everyone could exchange information, research data and utilize programs through interconnections across the world'.[16] It was this idea that was inherent in the ARPANET connection system, the predecessor of today's Internet.

Figure 2: Advanced Research Projects Agency (ARPA) network links 1969

Source: Introduction to computer science website [17]

Operation

In October 1972 the ARPANET system linking computers was first publicly demonstrated, and at the same time, electronic mail (email) between terminals was exhibited. In the 1970s, a networking protocol that would allow an open-architecture for multiple networks to be joined together—the Transmission Control Protocol/Internet Protocol or TCP/IP—was developed. The TCP/IP has been called the 'backbone protocol' which has determined what the Internet is.[18] The New Media Institute's history of the Internet explains that the TCP/IP:

15. J Strickland, 'How did the Internet start?', howstuffworks website, accessed 14 November 2013.
16. J Marx, 'History and facts about the Internet', eHow website, accessed 26 September 2013.
17. Illustration from 'Introduction to CIS', Introduction to computer science website, accessed 10 February 2014.
18. I Peter, 'History of the Internet', Net History website, accessed 8 April 2014.

> … would allow each individual network to stand alone such that if another network was brought down, it would not cause the collapse of all joined networks. Additionally, the new protocol … would involve no overall global manager and would join various networks together through what would later be known as routers and gateways. After the original TCP/IP protocol was written, what emerged as the Internet would result from ongoing experimentation and TCP/IP would emerge as an almost universal host protocol on which the Internet would be built.[19]

These developments were accompanied by suggestions that ordinary folk should be able to access computer and network technology, and proposals were made to 'hypertext' information to link it in a less linear manner. In 1976 Apple computers was founded, and by 1978, Apple had launched the first mass marketed personal computer.[20] In 1979, a program was developed that allowed files to be transferred between networked computers by way of a dial-up connection. This system was the genesis of what were called Bulletin Boards—the first attempt to create what has become the virtual community of the Internet.[21]

Box 1: the World Wide Web

Before the World Wide Web (the Web), the Internet only provided screens full of text (usually in one font and font size).

In attempting to make the Internet look more visually appealing, new concepts were conceived and developed and one of the most important of these was hypertext (hyperlinks), which was to become the foundation of the World Wide Web.

Another concept was the URL or Uniform Resource Locator, which became a unique address used by each web resource.

Yet another was Hypertext Markup Language (html), which allowed pages on the Internet to display different fonts and sizes, pictures and colours, and to link to documents and resources.

The first trials of the Web were in Switzerland in December 1990. By the end of 1992, there were about 26 sites on the Web.

Evolution of the Internet

The evolution of the Internet to a wider application was hastened by the spread of the Bulletin Board System (BBS) in the 1980s. The BBS enabled a computer with a special configuration to connect to telecommunications networks. Bulletin Boards allowed computer users to leave messages that could be read by other users of a particular system. Later, as Bulletin Boards became more sophisticated by using developments such as those noted in Box 1, they allowed users to download software and information to their personal computers.

By the early 1990s, most Bulletin Boards were connected to the Internet, and the Web was a reality; the connection of Bulletin Boards to the Net delivered information of all types to personal computers—information which included pornography and material of a violent nature.[22]

So it was that the evolution of the Internet went hand in hand with that of the personal computer. Through various iterations computers developed from large main frame devices for military and business applications to the smaller portable versions which are a feature in most homes today.[23] It was this combination—home computers giving broad access to information and the Internet which carried the information into individual homes—that created new censorship dilemmas for democratic governments.

Initially those dilemmas were limited to protecting the vulnerable members of the community from certain types of pornography and images of extreme violence. However, as technology has evolved, other threats have emerged to add to the dilemmas for governments. Now, hand-held devices with inbuilt cameras and 'app' based

19. New Media Institute (NMI), 'History of the Internet', NMI website, accessed 8 April 2014.
20. apple-history, 'Company history: 1976–1981', apple-history website, accessed 17 April 2014.
21. The BBS Corner, 'A brief history of BBS systems', the BBS Corner website, accessed 17 April 2014.
22. As the use of the Internet became more widespread, the Bulletin Board System (BBS) concept faded in popularity. Internet forums now occupy similar social and technological spaces. Note: the World Wide Web is a subset of the Internet. It consists of pages that can be accessed using a web browser. The Internet is the actual network of networks where all the information resides.
23. J Garger, 'A brief history of who invented the personal computer', Bright Hub website, 18 May 2011, accessed 10 July 2014.

software are the norm. People have instantaneous access to social media sites—such as facebook, twitter and snapchat—all the benefits of the Internet. But with the benefits come the disadvantages. Predators and unsavoury characters also have greater access to the means through which they can prey on unsuspecting citizens.

Technology will continue to evolve and this will impose greater demands on governments to protect business and the community. Cyber security efforts will need to be made to protect business networks from, amongst other things, increasing incidences of online piracy. For the community, the focus will need to be on interactive threats—online grooming of children, cyber bulling and more recently sexting, online fraud including the dangers of identity theft and the effects, in the national security context, of the spread of radicalising material.

In this context, governments will need to be even more aware of the difficulties they will face if they seek to impose any form of control.

The dilemma: balancing freedom and the potential for harm

As a report to the United Nations (UN) noted in 2011:

> Unlike any other medium the Internet facilitated the ability of individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an 'enabler' of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole.[24]

At the same time, the report acknowledged that like all technological inventions, the Internet can be misused to cause harm.[25]

A rights approach

Regulating the Internet has therefore presented an ongoing dilemma for the governments of countries which pride themselves on following liberal democratic principles—namely, to what extent should they attempt to regulate the Internet to prevent harm and what form should that regulation take. Governments see this dilemma as resolvable. The Dutch Government for example argues:

> As the primary entities responsible for the protection of the fundamental rights and freedoms of their citizens, governments play a central and crucial role in supplying open access to the Internet, guaranteeing internet freedom and securing the rule of law online.
>
> An open and free Internet is a key means by which individuals can exercise their right to freedom of opinion, expression, association and assembly. However, these freedoms are not absolute. In protecting and furthering internet freedom, governments must take account of the rights and interests of all members of society. The conduct of individuals, groups or institutions online may be at odds with the rights of others. Therefore, in furthering internet freedom, governments also have a duty to protect these rights and interests. These rights and interests include (cyber) security, the right to privacy, protection against speech that incites violence, and the dignity of individuals.[26]

Some commentators are less supportive of a role for government. One argues that government controls meant to deal with cybercrime and censoring online content 'open the doors to violations of human rights'.[27] In addition, government actions are likely to be ineffective because governmental structures are not swift or flexible enough to respond to cybercrime. Furthermore, in this commentator's view blocking and filtering technologies 'trigger the development of online tools that circumvent blocking programmes and government surveillance' and result in ever-increasing government spending to keep pace with criminals.

---

24. F La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Report to the United Nations' Human Rights Council, 16 May 2011, p 6, accessed 15 April 2014.
25. Ibid.
26. The Netherlands, Ministry of Foreign Affairs, *The role of governments in protecting and furthering internet freedom: background paper*, The Hague, Ministry of Foreign Affairs of the Kingdom of the Netherlands, n.d., accessed 15 April 2014.
27. M Le Pelley, *Champions of internet freedom ignore online ethics at their own peril*, Friedrich-Ebert-Stiftung, Berlin, January 2013, accessed 15 April 2014.

An economic approach

A paper from the Adam Smith Institute in the United Kingdom, on the other hand, considers that, with regards to the Internet, 'the freedom to be able to conduct business, engage with others and communicate freely should be fundamental to government policy, and should be safeguarded against regulatory restrictions'.[28] In the view of the author of this paper, advocates of website blocking to protect children forget that children who are at risk online are likely to be at risk offline.

> Vulnerability online is a symptom of deeper family problems, and cannot be addressed through simple website blocking, which only focuses on symptoms. We should be extremely concerned about the idea of a government official or committee deciding what people should and shouldn't be allowed online. How do these committee members know they are right? What knowledge do they possess about children over the knowledge of the family raising those children? And how can a committee decide what is best for each and every family? These are questions that advocates of website blocking cannot answer.[29]

It seems that for liberal democracies resolving the dilemma surrounding regulation of the Internet 'is a question of finding the right balance between sometimes diverging principles' so as to ensure security and public safety without overly restricting privacy and freedom of expression.[30]

Australia: initial response

Like many of its counterparts elsewhere, in the early 1990s the Labor Government was disturbed about the development of Bulletin Boards and the potential for users to post pornographic and/or violent materials on them.[31] As government clearly had power under the *Australian Constitution* to subject publications to the classification system, it tasked a Senate committee with examining the legal and technical issues involved with establishing an appropriate regime for Bulletin Boards and computer networks.

In October 1993, the Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies (SSCCS) concluded there were 'complex regulatory problems' involved as a result of the availability of unsavoury pornographic and other offerings on Bulletin Boards. The SSCCS urged state appointed censorship ministers 'to give consideration to immediate remedial measures'.[32] In response, in the following year, the Labor Government's Attorney-General, Michael Lavarch, and the Minister for Communications and the Arts, Michael Lee, initiated a taskforce to investigate the BBS phenomenon.[33]

Attorney-General Lavarch conceded from the outset that the area would be difficult to control:

> ... given that the technology is such that it makes regulation and any enforcement very problematic. Nonetheless, given the evidence that confronts ministers on this issue, it is incumbent upon the Commonwealth to examine what is hopefully an appropriate response.[34]

In a report on the BBS, the Regulation of Computer Bulletin Boards Taskforce (the Taskforce/Bulletin Boards taskforce) set up to investigate Bulletin Boards agreed that there were practical limits to their regulation.[35] Further, the Taskforce speculated that comprehensive government scrutiny could be costly, and importantly, that it could lead to accusations that government action impeded development of what had come to be referred

28. D Lazanski, *Internet freedom: a free market digital manifesto*, Briefing paper, Adam Smith Institute, London, n.d., accessed 15 April 2014.
29. Ibid.
30. Y Breindl and J Wright, 'Internet filtering trends in Western liberal democracies: French and German regulatory debates, paper presented to the 2012 Workshop on Free and Open Communications on the Internet (FOCI'12), Bellevue, Western Australia, 8 June 2012, accessed 15 April 2014.
31. M Lavarch, 'Answer to Question without Notice: Censorship', [Questioner: P Dodd], House of Representatives, *Debates*, 8 February 1994, p. 511, accessed 28 January 2014.
32. Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies, *Report on video and computer games and classification issues,* The Senate, Canberra, October 1993.
33. M Lavarch (Attorney-General), *Task force on computer bulletin boards*, media release, 3 February 1994, accessed 26 September 2013.
34. M Lavarch, 'Answer to Question without Notice: Censorship', op. cit.
35. Regulation of Computer Bulletin Boards Taskforce, *Regulation of computer Bulletin Board Systems*, Australian Government Publishing Service (AGPS), Canberra, 1995.

to as 'the information highway'.[36] At the same time, the Taskforce accepted that Australian censorship principles—adults should be able to see, hear and read what they want, while children should be protected from material likely to harm or disturb—could be applied to Bulletin Boards with the cooperation of operators. To achieve this aim, the Taskforce listed a number of options, but appeared to favour:

> … industry guidelines backed by a complaints mechanism which would not require legislation to implement initially, although continued monitoring [was] also recommended to establish whether failure to comply with the guidelines should be an offence.[37]

In a presentation to the Bulletin Boards Taskforce, the internet industry was wary that a possible consequence of regulating content at any level would be the inhibition of commercial development of the Internet.[38] Critics of the BBS report also considered that issues of privacy and free speech for BBS users had been 'glossed over' to the point where they were 'virtually invisible'.[39]

Thus, the questions surrounding regulation became more complicated. As well as asking whether content on the Internet should be subject to regulation, stakeholders had introduced the idea of whether content **could**, technically, be regulated. The Government's first reaction was to concentrate on the principles of regulation rather than the vehicles; that is, to favour technology neutral censorship, whatever the vehicle for carriage of information, the same classification system would apply.

In response to the Bulletin Boards Taskforce, the Attorney-General envisaged an approach to regulation of the Internet which consisted of three tiers:

- a code of practice developed by industry
- a complaints mechanism similar to that used in the telecommunications sector and
- legislation which would make it an offence to produce material for the Internet that would be banned if it were to be produced for film, video or literature or material that would receive a rating which would not allow it to be available to minors.[40]

With this direction in mind, in July 1995, the Government issued a consultation paper on the regulation of online services and the Australian Broadcasting Authority (ABA) was directed to investigate the content of online information and entertainment services.[41] In the following month, the SSCCS launched its own inquiry into the regulation of computer online services.

Prior to the 1996 election, the SSCCS expressed its support for a system of self-regulation, involving codes of practice and including an independent complaints body.[42] Following the election, an ABA report, which contained similar recommendations, was released.[43]

---

36. M Lavarch (Attorney-General), '*Computer bulletin boards task force report released*', media release, 5 October 1994, accessed 26 September 2013. Note: webopedia describes the term 'information superhighway' as a popular buzzword used to describe the Internet, Bulletin Boards, online services and other services that enable people to obtain information from telecommunications networks.
37. Lavarch, Computer bulletin boards task force report released, op. cit.
38. R Frawley (Manager, Internet Industry Association of Australia) and G Slater (Co-President, Internet Industry Association of Australia), *Public seminar on the regulation of bulletin board* systems, presentation to Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies*, Inquiry into the regulation of bulletin board systems*, 4 April 1995, accessed 26 September 2013.
39. K Auer (President, PC Users Group (ACT)), Public seminar, presentation to Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies, , op. cit.
40. M Lavarch (Attorney-General), 'Answer to Question without Notice: Internet rape guide' [Questioner: M Evans], House of Representatives, *Debates*, 19 June 1995, p. 1720, accessed 26 September 2013.
41. M Lavarch (Attorney-General) and M Lee (Minister for Communication and the Arts), *Content regulation of on-line information services*, media release, 9 July 1995, accessed 26 September 2013.
42. Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies, *Report on regulation of computer on-line services: part 2*, The Senate, Canberra, November 1995, accessed 26 September 2013. See also Senate Select Committee on Community Standards Relevant to the Supply of Services Utilising Electronic Technologies, *Report on regulation of computer on-line services: part 3*, The Senate, Canberra, November 1995, accessed 26 September 2013.
43. Australian Broadcasting Authority (ABA), *Investigation into the content of on-line services: report to the Minister for Communications and the Arts*, Sydney, 1996. A short summary of the report is available online.

The Howard Government: regulating the 'liberal' way

Broad framework

Not long after it took office in March 1996, the Coalition Government, led by John Howard, announced a set of fundamental principles which it intended to apply to regulation of the Internet. These reflected the direction towards which it appeared the previous government had been predisposed but, in the Coalition's case, with more stress on a preference for self-regulation. In a joint media release in mid-1997, the Attorney-General, Darryl Williams, and the Minister for Communications and the Arts, Senator Richard Alston, declared:

- material accessed through online services should not be subject to a more onerous regulatory framework than 'offline' material such as books, videos, films and computer games
- a framework for online services would need to balance community concerns in relation to content and at the same time ensure that regulation did not inhibit industry growth and potential and
- as Internet Service Providers (ISPs) were not aware of the kind of material transmitted through their services, they could not be held responsible in every case for material they had not created.[44]

By 1998, the ABA began to look at how regulatory arrangements for online services could operate within this broad framework. It released a consultation paper in July 1998 which incorporated the Government's preliminary policy statement with a proposal to set the legal and regulatory framework for the information economy.[45] Comments were sought on proposed actions to:

> … address community concerns about objectionable online content through a national industry-based regulatory scheme for service providers, a consistent State and Territory legislative framework to guide content providers, the promotion of content labelling and filtering technologies, and educational campaigns.[46]

In other words, it appeared the intention was that regulation of the Internet would follow the traditional pattern for media regulation in the Australian context—a basic industry self-regulatory regime, tempered with certain legislative requirements.

Some radical comments received in response to the ABA paper firmly branded such an approach for the Internet as hypocritical. As one group put it, the Government's 'expressed desire to regulate service and content providers fundamentally conflicts [with] its stated objective of allowing "unprecedented access" to information'.[47]

Following its re-election in October 1998, the Howard Government declared it would not tolerate the Internet being polluted by highly offensive or illegal material and it would do everything in its power to stop criminals preying on children.[48] At the same time, Minister Alston underlined a conviction that there were limits to the state's role:

> ... there is only so much that Governments can or should do [with regards to regulating the Internet]. We can crack down on illegal activity, and we can work with the industry to minimise potential problems, but we can't replace the guardianship role of parents.[49]

---

44. R Alston (Minister for Communications and the Arts) and D Williams (Attorney-General), *National framework for on-line content regulation*, media release, 15 July 1997, accessed 26 September 2013.
45. Ministerial Council for the Information Economy, *Towards an Australian Strategy for the Information Economy*, consultation paper, National Office for the Information Economy, Canberra, July 1998.
46. Ibid., p. 23.
47. Electronic Frontiers Australia, Submission to Senate Select Committee on Information Technologies, *Self-regulation in the Information and Communications Industries Inquiry*, 1998, accessed 26 September 2013 and Electronic Frontiers Australia, *A response to the Commonwealth Government's preliminary policy statement titled: towards an Australian strategy for the information economy*, 1998, accessed 26 September 2013.
48. R Alston (Minister for Communications, Information Technology and the Arts), *Alston launches vital new internet tool for parents*, media release, 27 November 1998, accessed 26 September 2013.
49. Ibid.

Box 2: types of internet filters

There are three distinct types of internet filters:

Blacklist or exclusion filters

Blacklist filters are the most popular types of internet blocking software. A website is added to a blacklist that keeps track of content with objectionable words and images. When a user tries to access the website address on their browser, the software compares the address to the addresses on the list. If there is a match, the users are denied access to the requested website.

White list or inclusion filters

White list filters allow access only to so-called good sites on a list, while denying access to websites not on the list. White list filters are the most restrictive blockers.

Keyword or content filters

Keyword or content list filters scan websites for the presence of specific words, phrases or images that appear on a restricted list and access to websites containing these is denied.

According to a Commonwealth Scientific and Industrial Research Organisation (CSIRO) report in September 2001, as inclusion filtering only allowed access to a relatively small number of acceptable sites, its main problem was that it blocked almost all content on the Internet. This was regardless of the acceptability of that content.[50] The disadvantage of exclusion filtering was that it allowed access to content on sites not on exclusion lists. Content filtering also had its limitations. For example, dubious content could be specified as graphics with large amounts of 'flesh tones', so not only would *Penthouse* centrefold sites be blocked, but sites including Rubens paintings could conceivably be unacceptable.[51]

Including a legislative component

Broadcasting Services Act amendments

Working within these limits, regulation which the Government had promised to introduce during the 1998 election campaign was developed in the form of a new schedule to the *Broadcasting Services Act 1992* (the *BSA*).[52] Schedule 5 to the *BSA* was introduced by the *Broadcasting Services Amendment (Online Services) Act 1999* (see an explanation of Schedule 5 in Box 2).[53] The Explanatory Memorandum to the originating Bill (Online Services Bill) reinforced the Government's overall policy stance. This was that while it took its responsibility to address the publication of illegal and offensive material on the Internet seriously, it did not wish to impose 'onerous or unjustifiable burdens on industry' in the process. Nor did it wish to inhibit the development of the online economy.[54] Hence, its proposed regulatory framework was intended to strike a balance between the interests of industry and those of the wider community.

The Explanatory Memorandum acknowledged that blocking illegal and offensive material which originated from overseas would be 'difficult'.[55] The Government was prepared in the first instance to leave this task to industry. Only if industry was then 'unable or unwilling' to develop procedures, or if procedures were found to be deficient, was it prepared to consider an option for the ABA to make a mandatory industry standard.[56]

50. P Greenfield, P Rickwood and Huu Cuong Tran, *Effectiveness of internet filtering products*, Report prepared for NetAlert and the Australian Broadcasting Authority, September 2001.
51. K Needham, 'Software nannies not always to be trusted', *The Sydney Morning Herald*, 27 March 2002, accessed 28 October 2013.
52. *Broadcasting Services Act 1992* (Cth) (BSA), Schedule 5, accessed 13 February 2014.
53. *Broadcasting Services Amendment (Online Services) Act 1999* (Cth), accessed 26 September 2013.
54. Explanatory Memorandum, Broadcasting Services Amendment (Online Services) Bill 1999, p. 2, accessed 26 September 2013.
55. Ibid., p.1.
56. Ibid., p. 2. Part 9B of the *Broadcasting Services Act 1992* provides that the Australian communications and Media authority (ACMA) has a reserve power to make an industry standard if there are no industry codes, or if an industry code is deficient. Compliance with industry codes is mandatory.

The Senate Committee on Information Technologies (SCIT) inquiry into the Online Services Bill appeared to be more inclined towards a legislative solution to tackling the publication of illegal and offensive material on the Internet:

> Self-regulation, even with the industry's stated best intentions, is not adequate. Without legislative pressure, there is no incentive for the industry to seek better, faster, cheaper ways of achieving the outcome apparently desired by the Australian Government on behalf of the Australian community—that its citizens are able to take control of what standards of content it wishes to accept in its media, irrespective of the means of delivery.[57]

But the Senate Committee was also patently aware that legislation would not solve the entire problem:

> Australian law can only cover content providers and ISPs which are operating within Australia's jurisdiction. Since the vast bulk of material emanates from offshore, outside Australia's jurisdiction, this legislation provides the only opportunity to deal with offensive material coming from overseas.[58]

While the majority of the SCIT recommended that the Online Services Bill should be passed without amendment, a minority report questioned the validity of the Government's claim that there was 'overwhelming community concern' about explicit sexual material on the Internet.[59] The report, by Australian Democrats' Senator Natasha Stott Despoja, argued that evidence suggested that the Australian public was more concerned about inappropriate censorship and extreme violence and racism than sexually explicit material on the Internet. Senator Stott Despoja also expressed concern that the Government was unwilling to address the civil liberties issues which were raised by the proposed legislation.[60]

Independent Senator Brian Harradine was also dissatisfied with provisions in the Online Services Bill. Senator Harradine argued that while the Bill was an improvement on an unregulated environment, it fell short of previous recommendations for stronger regulation. Moreover, Harradine questioned whether the 'passive' ABA had the ability to scrutinise complaints procedures in the legislation.[61]

Some of the relevant key features of Schedule 5 are shown in the box below:

57. Senate Select Committee on Information Technologies, *Broadcasting Services Amendment (Online Services) Bill 1999*, The Senate, Canberra, 1999, p. 11, accessed 4 February 2014.
58. Ibid.
59. N Stott Despoja, Minority report, Senate Committee on Information Technologies, Broadcasting Services Amendment (Online Services) Bill 1999, op. cit.
60. Ibid.
61. B Harradine, 'Qualifying comment', Senate Committee on Information Technologies, Broadcasting Services Amendment (Online Services) Bill 1999, op. cit.

Box 3: *Broadcasting Services Act 1992*: Schedule 5

Features of Schedule 5 of the *BSA* relevant to internet regulation included:

- a definition of 'internet content' intended to capture Bulletin Boards[62]
- classification of internet content based on the National Classification Board guidelines to ensure that it was classified in a corresponding way to the classification of film, videos or computer games under the Classification (Publications, Films and Computer Games Act) 1995[63]
- a definition of 'prohibited content'—that is, internet content (hosted in Australia) that has been classified Refused Classification or X or internet content that has been classified R where access to the content is not subject to a restricted access system[64]
- the ABA given power over 'potential prohibited content' (meaning internet content that has not been classified, but which, were it to be classified, was likely to be prohibited)[65]
- a complaints-driven regulation scheme allowing a person to complain to the ABA if he/she believes that an ISP is supplying a service that enables end-users to access prohibited content or potential prohibited content[66]
- where the ABA is satisfied that internet content hosted in Australia is prohibited, it must issue a notice directing the Internet Content Host (ICH) to the content and
- if material has not been classified and the ABA believes that there is a substantial likelihood that the content would be classified as RC or X, then the ABA must issue the ICH with an interim take-down notice and request the Classification Board to classify the internet content. A final take-down notice is to be issued if the internet content is found to be prohibited.

Industry code

The *BSA* amendments required the Internet Industry Association to develop a code of practice for ISPs (see Box 7 below) to provide for the use, at a charge determined by individual ISPs, of an approved filter to each of their customers.[67] A number of sources criticised the code because it was developed by a group which represented only a small number of ISPs.[68] Some believed the code was not sufficiently open and transparent and that sites blocked under the code would be kept secret and the blocked sites not informed they were being blocked.[69] Despite such concerns, the ISP Industry Code of Practice was approved by the ABA on 16 December 1999, and further revised in 2002 and 2005.[70]

In announcing the 2005 version of the code, the Minister for Communications, Senator Helen Coonan, welcomed initiatives taken by the industry which required ISPs to display a link to Internet safety information prominently on their home page and to provide customers with regular updates on filtering options every four months.[71] The 2005 code also introduced measures which attempted to deal with the increasing variety of means through which children could access offensive material including provisions for content delivered to multimedia-enabled mobile phones.[72] However, as information in Box 4 below illustrates, despite the best of intentions, it became

62. Clause 3, Schedule 5 of the *BSA*.
63. *Classification (Publications, Films and Computer Games Act) 1995* (Cth), accessed 26 September 2013.
64. Clause 3, Schedule 5 of the *BSA*.
65. Note: the ABA merged with the Australian Communications Authority on 1 July 2005 to form the Australian Communications and Media Authority (ACMA). ACMA is responsible for the regulation of broadcasting, the Internet, radiocommunications and telecommunications.
66. Clauses 23–25, Schedule 5 of the *BSA*.
67. R Alston (Minister for Communications, Information Technology and the Arts), *Government welcomes Internet code of practice*, media release, 16 December 1999, accessed 26 September 2013. Note: it was not required for an ISP to supply a filter if a customer had already installed such a filter.
68. The Libertus website cites the Telecommunications Ombudsman's figures for 1999 as a source for this claim, accessed 11 July 2014.
69. Electronic Frontiers Australia, *Net censorship: secret and unaccountable*, media release, 1999, 19 December 1999, accessed 11 July 2014.
70. Australian Communications and Media Authority (ACMA), Online codes, ACMA website, accessed 11 Jul 2014.
71. H Coonan (Minister for Communications, Information Technology and the Arts), *Making the Internet safer for families*, media release, 27 May 2005, accessed 26 September 2013.
72. Ibid. and current Internet Industry Association codes, accessed 10 February 2014.

increasingly clear that regulating the online world and protecting children from inappropriate material posed, and most likely will continue to pose, unexpected challenges.

Box 4: ephemeral content

As the online world has developed, so more issues of concern for those who seek to regulate it have arisen. The regulation of ephemeral content (that is, essentially live content) has been one of these. Ephemeral content includes streamed audio visual material and interactive chat services.

In 2006, for example, controversy surrounded the showing of live content associated with the *Big Brother* television show.[73] Existing media regulation ensured that an incident, in which two male contestants allegedly sexually harassed a female contestant, was not shown on television.[74] However, existing online content regulation was unable to prevent streaming on the Internet of video of the incident through *Big Brother*'s website.[75]

Senator Coonan described the incident as 'disturbing and offensive and many in the community are rightly concerned by the prospect of footage of this incident being broadcast'.[76] The incident prompted the Government to introduce legislation which was intended to ensure that children would not be exposed to inappropriate or harmful material or lured into unsafe contact as a result of accessing ephemeral content.[77]

Whilst Labor confirmed its support for the amending legislation, Senator Conroy voiced concerns that it would 'not protect children from accessing inappropriate or harmful material from sites hosted in countries other than Australia'.[78]

NetAlert

The 1999 online services legislation, which introduced Schedule 5 to the *BSA*, also allowed for the establishment of a community advisory body to monitor on the Internet and to educate communities about managing access to online content. This body, NetAlert, commenced operations in November 1999.[79] NetAlert initially developed a website and toll free national help line, but during 2007 it evolved to include a more comprehensive range of measures under the Protecting Australian Families Online program. In August 2007, Senator Coonan announced that the program would include:

- a National Filter Scheme to provide access to the internet filtering technology free to every Australian family (see information on types of internet filters in Box 4). Families were to have a choice between a PC-based filter for installation on their home computer or an ISP-filtered internet service, either of which would filter web content against an ACMA blacklist (see explanation in Box 5 below) and
- filtering for all public libraries.[80]

73. P Dockrill, 'Big brother turkey slap controversy threatens net freedom', *APC*, 6 July 2006, accessed 27 September 2013.
74. Under section 123 of the *BSA*, industry groups have developed codes of practice in consultation with ACMA. Once implemented, ACMA monitors these codes and deals with unresolved complaints made under them. Under paragraph 1.9.7 of the *Commercial Television Industry Code of Practice 2010*, a licensee may not broadcast a program which is likely, in all the circumstances, to present participants in reality television programs in a highly demeaning or highly exploitative manner. The term 'demeaning' refers to a depiction or description, sexual in nature, which is a serious debasement of a person, or a group of persons, within a program.
75. B Jaggers, M Neilsen and R Jolly, *Communications Legislation Amendment (Content Services) Bill 2007*, Bills digest, 158, 2006–07, Parliamentary Library, Canberra, 23 May 2007, p. 6, accessed 26 September 2013.
76. H Coonan (Minister for Communications, Information Technology and the Arts), *'Big Brother'*, media release, 5 July 2006, accessed 27 September 2013.
77. H Coonan (Minister for Communications, Information Technology and the Arts), *Review of the Television Code of Practice and the regulation of online content*, media release, 5 July 2006, accessed 26 September 2013. The relevant legislation is the *Communications Legislation Amendment (Content Services) Act 2007* (Cth), accessed 27 September 2013.
78. S Conroy, 'Second reading speech: Communications Legislation Amendment (Content Services) Bill 2007', Senate, *Debates*, 20 June 2007, p. 133, accessed 26 September 2013.
79. R Alston (Minister for Communications, Information Technology and the Arts), *Internet content advisory board announced*, media release, 26 November 1999, accessed 26 September 2013.
80. H Coonan (Minister for Communications, Information Technology and the Arts), *NetAlert: protecting Australian families online*, media release, 10 August 2007, accessed 26 September 2013; and H Coonan (Minister for Communications, Information Technology and the Arts), *NetAlert's comprehensive internet safety programme*, media release, 27 August 2007, accessed 26 September 2013.

Box 5: about the ACMA blacklist

ACMA has no power to direct the removal of prohibited content and potential prohibited content hosted outside Australia. Instead, Schedule 5 to the *BSA* sets up a system for regulating certain aspects of the internet industry whereby if ACMA is satisfied that internet content hosted outside Australia is prohibited content or potentially prohibited content, it must:

- notify the content to an Australian police force if it considers that the content is of a sufficiently serious nature to warrant referral to a law enforcement agency and
- notify the content to ISPs so that they can deal with the content in accordance with procedures specified in industry codes or industry standards (for example, procedures for the filtering, by technical means, of such content). [81]

To comply with this requirement, ACMA notifies the URLs of prohibited content and potential prohibited content hosted outside Australia to the makers of certain filter software products, which Australian ISPs are required to offer to their customers. [82]

The ACMA blacklist, which started to be compiled in 2000, is the list of URLs of prohibited content and potential prohibited content maintained by ACMA as part of its regulatory responsibilities for online content under Schedule 7 of the *BSA*. ACMA's current list contains approximately 1,110 URLs covering material in the following categories:

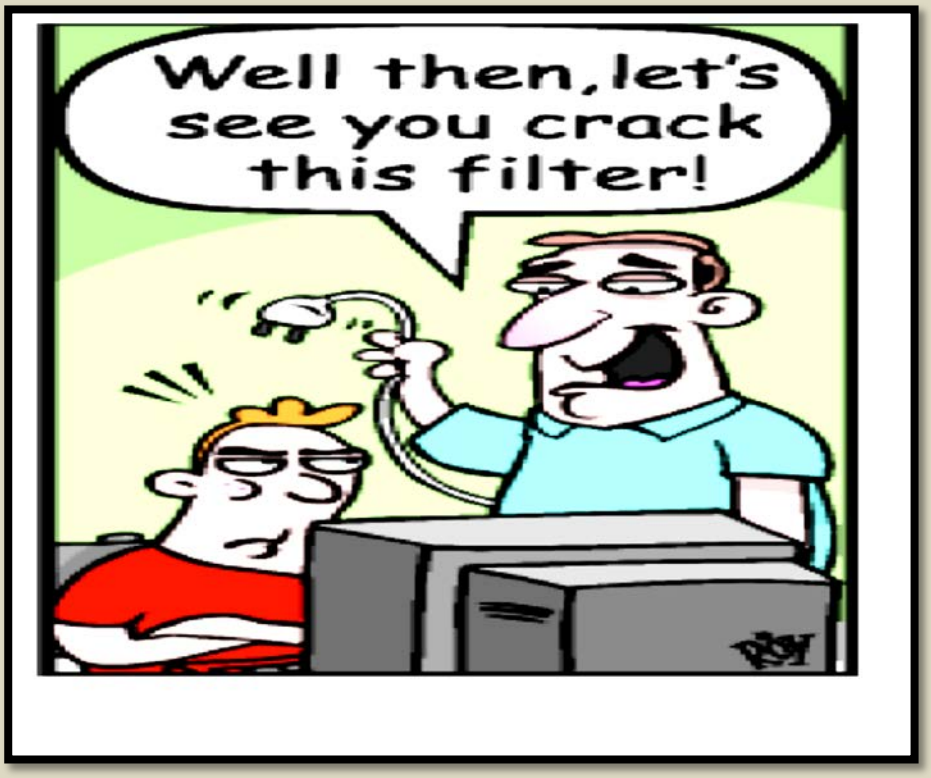
- depictions of child sexual abuse
- depictions of bestiality
- material containing excessive violence or sexual violence
- material containing detailed instruction in crime, violence or drug use
- real depictions of actual sexual activity and depiction of simulated sexual activity which is not subject to a restricted access system. [83]

The Opposition Communications spokesperson, Senator Stephen Conroy, welcomed the Government's announcement of these measures, but still believed the Government should go further and mandate ISP level filtering. Internet experts warned that the Government's $84.8 million package was no 'silver bullet', and even the Government admitted that 'net-smart kids could get around any measures their parents put in place' (see comment in Box 6 below).[84]

81. Clause 2 of Schedule 5 to the *BSA*.
82. ACMA, *'Blacklist' of prohibited websites published online*, media release, 19 March 2009, accessed 27 September 2013.
83. ACMA, *Online content complaints: fact sheet*, 22 May 2014, accessed 27 September 2013.
84. S Conroy (Minister for Broadband, Communications and the Digital Economy), *Government welcomes ACMA report on internet filtering*, media release, 21 February 2008, accessed 10 February 2014.

Box 6: NetAlert: foiled or bypassed?

The day after Minister Helen Coonan launched the NetAlert filter package it was reported that Tom Wood, a Melbourne schoolboy, had disabled the filter in just over thirty minutes. Sixteen-year-old Wood showed reporters how to deactivate the filter while leaving an impression for parents that it was still working.[85] Some critics, including Family First Senator, Steve Fielding, a long-time campaigner for stronger filtering measures, saw this incident as proof that compulsory filtering by ISPs was required.[86]



Source: Herald Sun[87]

You can't please all the people

Doing too much

The Howard Government's approach to regulation of the Internet attracted a number of zealous critics. In May 2001, Greg Taylor, Vice Chair of the online civil liberties group Electronic Frontiers Australia (EFA), claimed the Government's regulatory scheme was expensive and inefficient. According to Taylor:

> The internet [sic] regulatory regime cost taxpayers about $2.5 million in its first full year, yet in the second half only six complaints related to local sites.
>
> [In relation to the Internet Content Regulation report for July to December 2000] … although 290 complaints were received during the six months, only 139 were found to relate to prohibited content and, of these, only six were found to be hosted locally …there seemed to be a massive waste of public money, with more than $1 million being spent on the ABA system, and about $1.5 million on the NetAlert program, for no obvious benefit.
>
> There's certainly nothing in the report that indicates NetAlert's usefulness to the community. Its main activity seems to have been promoting itself through widespread distribution of fridge magnets … the reporting of the scheme was designed to confuse, and the outcomes did not justify the cost.[88]

85. N Higginbottom and B Packham, 'No safety net', *Herald Sun*, 25 August 2007, p. 3, accessed 10 February 2014.
86. 'Internet filter not cracked: Coonan', *The Canberra Times*, 8 September 2007, p. 15, accessed 10 February 2014.
87. Ibid.

In 2005, EFA claimed further that the 'tough' internet regime had simply meant that pornography sites moved overseas. Executive Director of EFA, Irene Graham, criticised the internet regime put in place by the Howard Government because she believed it did not do what the Government intended—that is, it did not protect children from hardcore pornography and graphic violence. In addition, it prevented adults from seeing content 'that was freely available in other media'.[89] According to Graham, the law ensured that Australian businesses lost out as Australians used overseas sites to access adult content.[90]

In the weeks before Parliament was prorogued for the 2007 election, the Government introduced the Communications Legislation Amendment (Crime or Terrorism Related Internet Content) Bill 2007 to amend the *BSA* to expand the blacklist of internet addresses maintained by ACMA to include terrorism and cyber-crime websites hosted domestically and overseas.[91] Critics of this Bill argued that as it required ISPs to block access to overseas sites blacklisted by the Australian Federal Police Commissioner it could therefore 'inadvertently block access to popular sites such as Facebook and slow internet speeds to a snail's pace'.[92]

Not doing enough

In 2003, Clive Hamilton and Michael Flood of the Australia Institute argued from the opposing perspective that the Government was not doing enough to block unsavoury sites and those sites continued to be available to children on computers in homes and schools across Australia. Hence, children could inadvertently access inappropriate material. According to these critics, the co-regulatory scheme for the Internet was not working, despite claims to the contrary by the ABA and the Minister for Communications, Senator Alston. Hamilton and Flood put their view emphatically:

> ... the fact is that tens of thousands of websites showing pornography, some of it of the most extreme kind, are easily accessed by children. Not only is regulation of pornography on the Internet manifestly failing, but the regulatory authorities themselves appear to have lost sight of their functions. The ABA seems to be more concerned to promote use of the Internet than to protect children from its dangers.
>
> The same is true of the activities of NetAlert, the body established in the 1999 amendments to the Broadcasting Services Act to promote safe use of the Internet. It claims to have been highly successful and even proposes to change its name from NetAlert to 'Growing Australia Online' in order 'to remove the "alarmist" element' from its name, a conclusion it has reached after feedback from the Internet industry in discussions about 'cash and in-kind sponsorships'. NetAlert wants to redraft its charter so that there is no reference in its vision or goals to the dangers confronting young people in using the Internet.[93]

A broader alternative strategy

Hamilton and Flood proposed an alternative strategy to resolve the issue. This consisted of three components:

- a schools-based educational program to teach high school children to take a more detached and evaluative view of pornographic images and messages
- an opt-out system of ISP filtering and
- additional measures to protect children from exposure.[94]

These researchers considered that a more effective way of regulating the Internet would be to require Australian ISPs to filter all content, but to allow end users an option of requesting that content to their computer was not filtered. Additional measures to ensure that children would not be exposed to, or harmed by pornographic materials, would involve age verification, 'plain brown wrappers' for pornographic websites and help functions

88. K Dearne, 'Net censorship a $2.5m "waste"', *The Australian*, 15 May 2001, accessed 26 September 2013.
89. L Murray, 'Censors come calling', *The Sydney Morning Herald*, 23 September 2006, p. 38, accessed 27 September 2013.
90. S Hayes, 'Net law pushing sex sites overseas', *The Australian*, 26 July 2005, p. 33, accessed 26 September 2013.
91. Information about the Bill as introduced, the Explanatory Memorandum and the second reading speeches is contained on the homepage for the Communications Legislation Amendment (Crime or Terrorism Related Internet Content) Bill 2007.
92. K Dearne, 'Critics slam Canberra net block plan', *The Australian*, 25 September 2007, p. 31, accessed 27 September 2013.
93. M Flood and C Hamilton, *Regulating youth access to pornography*, Discussion paper no. 53, Australia Institute, 2003, p. v, accessed 26 September 2013.
94. Ibid., p. vi.

for children who had been exposed to pornographic material. A version of the latter suggestion for help functions has since been adopted with the introduction of features such as the Cybersafety Help Button introduced by the Labor Government (see more detail later in this paper). The Cybersafety Help Button provides advice for young people and families on how to handle cyberbullying or unwanted contact.

Hamilton and Flood also cited Thornburgh and Lin's suggestions for age verification techniques, such as the use of public records to authenticate age, 'smart cards' and age-tagged credit cards, as options.[95] They acknowledged that no system would be foolproof. However, if children were able to access restricted material as a result of bypassing an age verification system under such a system, it would not be because material had been refused classification—unless such material had escaped filters at an ISP. In addition, plain brown wrappers on 'sex' websites would ensure that no sexual imagery was displayed on opening pages of sites. Instead, a warning about the content behind the front page would be prominent. Finally, a function could be installed on computers for children who are subject to unwanted sexual solicitation or who are sent unwanted sexual material to assist them to seek help.[96]

Hamilton and Flood were aware that their proposals would restrict the commercial interests of ISPs and the civil liberties of internet users, but they saw any impositions as 'a small price to pay' given the potential for harm to children posed by unsavoury and predatory internet sites.[97]

They considered there is 'widespread but subterranean recognition' among Australians that pornography is potentially dangerous, but at the same time ordinary people feel reluctant to act or express concern for fear that they will be ridiculed as conservative or prudish. They concluded:

> Almost everyone agrees that depictions of rape, bestiality and sexual torture are sick, but no-one other than those seen to be moral fundamentalists is willing to admit their concerns ... Resolute measures to restrict young people from accessing pornography, and restrictions on the type of content that adults may see, do not imply a return to a pre-1960s era of sexual repression. Nor does conceding that some of the concerns of moral fundamentalists have a sound basis mean that one must share their worldview ... It seems to us that the clamour of moral fundamentalism reflects enough community concern for political leaders to want to be seen to be taking action, but that the equal and opposite fear of being drawn into some sort of moral dark age has meant that measures to restrict Internet pornography have been in large measure tokenistic. How else can one explain the position of the Federal Government and the regulatory authorities who declare that the system is working yet must be aware that five minutes of surfing the Internet will prove that it is, in fact, next to useless?[98]

Labor: a more paternalist approach?

A clean feed

It appears that Labor's thinking on internet filtering may have been influenced to some extent by the approach elaborated upon by Hamilton and Flood. Certainly, in the lead-up to the 2007 election, Labor announced that, if it were elected to office, it intended to take a different approach than that adopted by the Howard Government. According to Labor's communications spokesperson, Senator Stephen Conroy:

> 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 black list 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

95. Cited as Thornburgh and Lin, 2002, in text which it appears may be a chapter in D Thornburgh and S Herbert, eds, *Youth, pornography, and the Internet*. National Academy Press, Washington, D.C., 2002.
96. Flood and Hamilton, op. cit.
97. Ibid.
98. Flood and Hamilton, op. cit., p. 26.

and Online Protection (CEOP) Centre and ISPs to ensure that adequate online protection is provided to Australian children and families.[99]

Labor's policy was to require ISPs to filter out all material which would generally be refused classification or classified as X18+ under the National Classification Code[100] which is made in accordance with the *Classification (Publications, Films and Computer Games) Act*.

Under the classification system inherited by Labor, publications, films and computer games were refused classification if they:

- described, depicted, expressed or otherwise dealt with matters of sex, drug misuse or addiction, crime cruelty, violence or revolting or abhorrent phenomena in such a way that they offended against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified or
- described or depicted in a way that was likely to cause offence to a reasonable adult, a person who was, or appeared to be, a child under 18 years (whether the person engaged in sexual activity or not) or promoted, incited or instructed in matters of crime or violence.[101]

Films which were classified as X18+ contained real depictions of sexual activity between consenting adults. This activity involved no violence, sexual violence, sexualised violence, coercion, sexually assaultive language or fetishes or depictions which purposefully demeaned anyone involved in a way that was likely to cause offence to a reasonable adult. Films so classified were unsuitable for a minor to see.[102]

See the table below for an explanation of how these conditions applied differently to publications, films and games.

Table 1: classification system inherited by Labor

Publications[103]	**Films**[104]	**Computer Games**[105]
Unrestricted	G (General)	G (General)
Category 1 restricted	PG (Parental guidance)	PG (Parental guidance)
Category 2 restricted	M (Mature)	M (Mature)
Refused classification	MA15+ (Mature accompanied)	MA15+ (Mature accompanied)
	R18+ (Restricted)	RC (Refused classification)
	X18+ (Restricted)	
	RC (Refused classification)	

Source: *Classification (Publications, Films and Computer Games) Act 1995*[106]

99. S Conroy (Shadow Minister for Communications and Information Technology), *Labor's plan for cyber-safety*, Australian Labor Party policy document, Election 2007, 19 November 2007, accessed 26 September 2013.
100. National Classification Code, accessed 31 July 2014.
101. *Guidelines for the Classification of Publications 2005*, p. 14, accessed 7 November 2013.
102. *Guidelines for the Classification of Films 2012*, accessed 7 November 2013.
103. Classification (Publications, Films and Computer Games) Act 1995 (Cth), subsection 7(1).
104. Ibid., subsection 7(2).
105. Ibid., subsection 7(3). Under subsection 5B(2), five types of computer game are exempt from the requirement for classification—business, accounting, professional, scientific and educational games.

The commentary in relation to this policy showed the same polarity of views as had been apparent during the Howard Government era. On one side of the debate, the Chair of EFA, Dale Clapperton, opined that the internet filtering systems were 'too unreliable and gave the government too much power to control what adults could view online'.[107] On the other hand, Family First Senator Steve Fielding, who had campaigned for ISP filtering, stated that 'Australian families want more [Internet protection] and deserve more than they are currently getting' (as the cartoon below appears to indicate).[108]

Sorting out the filter

Could accurate filtering be achieved?

Labor won the 2007 election and while it remained committed to mandatory ISP filtering, its response to a February 2008 ACMA report indicated that it had come to the conclusion that regulation alone would not protect people from criminals and predators using the Internet.[109] According to Senator Conroy, who was the new Minister in a renamed Department of Broadband, Communications and the Digital Economy, the ACMA report identified:

> … that there is no silver bullet solution to the problem of online risks, especially as there is a shift from webpages to interactive internet technologies, such as chat rooms.
>
> The Government and the ACMA report also agree on the importance of education, and information and empowering people to manage online risks. A large component of the Government's cyber-safety plan is raising awareness of online safety issues and providing information on the strategies that can be undertaken to mitigate against these risks.
>
> The Government's cyber-safety plan presents a comprehensive range of measures that involves education, international co-operation, research, law enforcement and internet service provider (ISP) filtering.[110]

This more measured approach still did not please the industry, which was not convinced it was technologically feasible to filter the Net in the manner proposed by Labor. The Internet Industry Association (IIA) believed that there would always be 'technically savvy' people who will 'circumvent any and all filtering mechanisms'.[111] Hence, it was extremely difficult to stop all undesirable content on the Internet. It was better therefore to adopt goals to inhibit inadvertent access to undesirable content. The IIA continued to advance the argument that there were significant technical problems surrounding dynamic content filtering and its implementation in a nationwide ISP-based content filtering system. Therefore dynamic filtering was not a viable option for mandatory filtering. Because of inherent problems with the accuracy of filtering, mandatory filtering could be used only in opt-in frameworks. In opt-in frameworks, end users essentially agree to the possibility of some content being incorrectly classified, thereby removing responsibility from any third party provider.[112]

Filter testing

In July 2008, Senator Conroy released the findings of an ACMA report on extensive laboratory testing of the effectiveness of commercial ISP filtering products.[113] The report appeared to contradict the IIA view, stating that the products tested exhibited high levels of successful blocking of materials that should be blocked and low levels of blocking material which should be accessible.[114] The success of the closed testing led to live filter

---

106. *Classification (Publications, Films and Computer Games) Act 1995* at October 2007, accessed 6 November 2013. Broken link
107. A Colley, 'IIA ready for new internet censor battle', *The Australian*, 11 December 2007, p. 30, accessed 9 October 2013. permalink
108. *Protecting children from pornography*, Family First policy document, Election 2007, 1 October 2007, accessed 27 September 2013; and L Heywood, 'Porn filter may slow internet', *Herald Sun*, 31 December 2007, p. 4, accessed 27 September 2013.
109. ACMA, *Developments in internet filtering technologies and other measures for promoting online safety*, ACMA, Belconnen, ACT, February 2008, accessed 26 September 2013.
110. S Conroy (Minister for Broadband, Communications and the Digital Economy), *Government welcomes ACMA report on internet filtering*, media release, 21 February 2008, accessed 26 September 2013.
111. Internet Industry Association, *Feasibility study: ISP level content filtering*, February 2008, p. 9, accessed 8 October 2013.
112. Ibid, p. 12.
113. S Conroy (Minister for Broadband, Communications and the Digital Economy), *Minister welcomes advances in internet filtering technology*, media release, 28 July 2008, accessed 26 September 2013.
114. ACMA, *Closed environment testing of ISP-level internet content filtering*, ACMA, Belconnen, ACT, June 2008, accessed 26 September 2013.

testing being undertaken by six ISPs from February 2009.[115] The findings of this testing, which concluded in October 2009, were that all participants were successful in blocking 100 per cent of the ACMA blacklist, without performance degradation.[116]

On the other hand, the test report conceded that 'a technically competent user could, if they wished, circumvent the filtering technology'.[117] Similarly, while the results of the live pilot were an improvement on previous testing, it was considered that complete accuracy was 'unlikely to be achieved as the content on different commercial lists varies and there is a high rate at which new content is created on the internet'.[118]

These caveats on the live pilot findings did not deter the Minister from announcing in December 2009:

- introduction of mandatory ISP-level filtering of Refused Classification (RC)-rated content
- a grants program to encourage ISPs to offer, on a commercial basis, additional optional ISP-level filtering services for wider categories of content identified by households and
- increased funding for a range of education, awareness and counselling services.[119]

Box 7: ISP industry code of practice

While the live filtering pilot was underway, Senator Conroy announced the beginning of consultation on an ISP industry Code of Practice for e-security stating:

> An industry Code was a key recommendation of the E-security Review. The Code aims to provide a consistent approach for ISPs to help inform, educate and protect their customers in relation to e-security issues.
>
> The Code will also provide a framework for ISPs to inform clients about compromises on their computers and how they can address them.
>
> But in the main, the Code of Practice will be developed by ISPs for ISPs and their customers, with input from other relevant stakeholders.[120] This code of practice, as developed, applies to ISPs (as defined in Schedule 5 to the BSA). It is a voluntary code which is designed to provide a consistent approach for Australian ISPs to help inform, educate and protect their customers in relation to cyber security risks.[121]

Mounting opposition to the filtering proposals

Despite Labor's assurances that internet filtering was about providing safety, opposition to the Government's proposals continued to mount and a survey by the Internet discussion group, Whirlpool, in 2009 reported:

> … scant support for the federal government's proposed ISP-level mandatory internet filtering scheme, with just 7.4% of those polled backing the idea in principle against 92.6% opposed to the idea. Additionally, 44.1% cited the introduction of mandatory filtering as having an impact on their voting choices at the next federal election. Nevertheless, Whirlpool also noted surprisingly positive expectations of the filter's capabilities. 39.7% of respondents said they did believe the scheme could achieve its aim of restricting access to child pornography and 31.3% shared the opinion that it could protect children from harm.[122]

While the results of Whirlpool's survey may have been overly influenced by its constituency, the argument from leading web businesses, such as Google and Microsoft, that the scheme would have detrimental effects on

115. Primus Telecommunications, Tech 2U, Webshield, OMNIconnect, Netforce and Highway 1.
116. Enex testlab, *Internet service provider (ISP) content filtering pilot report*, Enex, October 2009, accessed 16 October 2013.
117 Ibid., p. 2.
118 Ibid.
119. S Conroy (Minister for Broadband, Communications and the Digital Economy), *Measures to improve safety of the internet for families*, speech, 15 December 2009, accessed 26 September 2013.
120. S Conroy (Minister for Broadband, Communications and the Digital Economy), *National E-security Awareness Week ISP Forum*, speech, 10 June 2009, accessed 26 September 2013.
121. Internet Industry Association, *Internet Industry Code of Practice*, 1 June 2010, accessed 16 October 2013.
122. P Wilton, 'Whirlpool survey finds strong opposition to filter', *Communications Day*, 3703, 8 March 2010.

speeds on the Internet was deserving of examination. Google and Microsoft contended also that there was a 'significant risk' that future governments could extend filtering to other forms of expression.[123] Other opposition to the scheme took a similar tack, questioning how far would the scheme allow the balance between freedom and restricting harmful internet content to tip. Colin Jacobs from EFA, for example, commented:

> In Australia, we sometimes hear politicians say something like, "We censor books and movies. Why should the internet be any different?" If you stop and think about it, it's not a difficult question to answer. The internet is fundamentally different. It's not just an electric newspaper or a virtual newsagent. It's huge. It's dynamic. It's global. Most importantly, it's about ordinary people communicating.
>
> When a book or a movie is censored, you're censoring a publisher or media company. They know how to navigate the classification system. They have lawyers to deal with that. And when a decision goes against them, it's public information. They can appeal.
>
> On the internet, the authors and publishers of the content are you and I. Everybody who has ever done so much as comment on a blog is an author, publisher and worldwide distributor of content. Censoring the internet for the first time in Australia brings the burden of censorship down on the average citizen's everyday discourse. That's a fundamental shift.[124]

Some commentators began to imply that Australia would be the first Western democracy to join China, Iran and other restrictive regimes if Senator Conroy's filter became reality.[125] Given the reputation of what has been termed 'China's Great Firewall' for prohibiting the likes of Twitter and censoring Google (see Box 8), it was likely this comparison was effective in influencing people's thinking about the proposed filter.

Tony Smith, Shadow Minister for Broadband, Communications and the Digital Economy, set out the Coalition position. It supported measures to protect children from inappropriate internet content but believed that this should be in the form of appropriate adult supervision and guidance.[126] Opposition Treasurer, Joe Hockey, added:

> What we have in the government's internet filtering proposals is a scheme that is likely to be unworkable in practice … but more perniciously it is a scheme that will create the infrastructure for government censorship on a broader scale.[127]

123. A Sharp, 'Google spots holes in internet filter plans', *The Sydney Morning Herald*, 24 March 2010, p. 5, accessed 28 October 2013; .J Bajkowski, 'Internet filter plan faces web backlash', *The Australian Financial Review*, 17 December 2009, p. 40, accessed 28 October 2013;M Sharma and P Koh, 'Web filter will compromise NBN, say providers', *The Australian*, 17 December 2009, p. 3, accessed 28 October 2013; R MacKinnon, 'Censorship is alive in the free world', *The Age*, 16 January 2010, p. 7, accessed 28 October 2013.
124. C Jacobs, 'The future of internet censorship', Electronic Frontiers Australia, 21 September 2010, accessed 12 February 2014.
125. M Kamenev, 'First, China. Next: the Great Firewall of... Australia?'**,** *Time*, 16 June 2010, accessed 12 February 2014.
126. T Smith (Shadow Minister for Broadband, Communications and the Digital Economy), *Mandatory internet filtering*, media release, 15 December 2009, accessed 28 October 2013.
127. A Sharp, 'Opposition grows to internet filter', *The Sydney Morning Herald*, 25 February 2010, p. 25, accessed 9 October 2013; and A Sharp, 'Web filter splits opposition', *The Age*, 7 April 2010, p. 10, accessed 9 October 2013.

Box 8: Internet censorship in China

The OpenNet Initiative noted in a 2004–05 study of access to the Internet in China that the filtering regime in that country:

> … is the most sophisticated effort of its kind in the world. Compared to similar efforts in other states, China's filtering regime is pervasive, sophisticated, and effective. It comprises multiple levels of legal regulation and technical control. It involves numerous state agencies and thousands of public and private personnel. It censors content transmitted through multiple methods, including Web pages, Web logs, on-line discussion forums, university bulletin board systems, and e-mail messages.[128]

The Economist explains that the Chinese central government employs two main controls on what its citizens see on the web: what foreigners have labelled 'the Great Firewall', which limits access to foreign websites, and the Golden Shield, which involves domestic surveillance.[129]

In 2006, in exchange for the right to install equipment in China, Google agreed to block websites which the Chinese government deemed illegal. However, in March 2010, Google began routing Chinese Internet users to its Hong Kong site as it said it would no longer comply with China's censoring policies and wouldn't run a censored Chinese search engine. In response, 'the Great Firewall' was used in 2010 to block it.[130]

In May 2012, Google announced an anti-censorship feature (which notified Chinese users when key words they were searching for would trigger the country's Great Firewall content blocking system). However, in December 2012, Google removed the feature, without informing its users, under the pretext of improving search quality—leading one journalist to label Google's actions an act of cowardice.[131]

Source: Nicholson[132]

The Greens voiced their concerns about Labor's intentions. Senator Scott Ludlam considered it 'the thin end of the wedge' that the Government expected that it would impose overseas blacklists to supplement the Australian list of banned websites.[133] On this point, the *Age* newspaper eloquently summarised the ongoing debate opining:

128. OpenNet Initiative, *Internet filtering in China 2004–05: a country study*, April 2005, accessed 12 February 2014.
129. 'How does China censor the Internet?', *The Economist*, 21 April 2013, accessed 12 February 2014.
130. J Vascellaro and L Chao, 'Google runs into China's "Great Firewall"', *The Wall Street Journal*, 31 March 2010, accessed 12 February 2014.
131. M Wright, 'Google shows China the white flag of surrender', *The Telegraph* (UK), 7 January 2013, accessed 12 February 2014.
132. 'The net in China', Nicholson cartoons, accessed 12 February 2014.
133. S Ludlam (Greens spokesperson), *Net filter report signals trouble ahead*, media release, 15 December 2009, accessed 28 October 2013; and A Moses, 'Big Brother laws to be brought in for web', *The Age*, 16 December 2009, p. 7, accessed 28 October 2013.

> The list of banned websites is to be maintained by an independent body 'at arms' length from the Government', yet the Government will add sites containing "known child-abuse material" obtained from "highly regarded international agencies". If the agency charged with this task is to be genuinely independent, why cannot it maintain the necessary content with "highly regarded agencies" itself? A body whose list can be topped up as and when the government of the day sees fit to do so hardly has an independence worthy of the name.
>
> Worse, the list is to be "compiled by a public complaints mechanism", which raises the prospect that innocent individuals may be denounced by those with hidden agendas, or that works of artistic or literary merit may be proscribed because of agitation by activists. *The Age* has noted before that distinguishing art from pornography is not the simple task self-proclaimed defenders of artistic freedom, or of public morals, sometimes assume it to be. However the line between them is to be judged, it is perilous for a liberal democracy to rely in these matters on what amounts to a clamour in the street.[134]

The press also took the opportunity to lampoon the filter in a number of cartoons, such as the one shown in Figure 3 below.

During January and February 2010, in undertaking 'Operation Titstorm', the group Anonymous added their voice to the protests by launching attacks against government and government-connected websites, including the Australian Parliament House website.[135] Pornography was also posted on the Prime Minister's homepage.[136] A spokesperson for Minister Conroy labelled the attacks as illegitimate and irresponsible, and according to one journalist, the Government was unmoved by either criticisms or protest, seemingly convinced that its policy was sound.[137] Another commentator believed this was because:

> Labor's private polling on internet filtering has consistently shown that a large number of computer-illiterate mums and dads are worried about what their kids can access online. They want [Senator] Conroy to make it safer for them.
>
> This is the reason he has continued to withstand so much virulent criticism from those who do not live in a nuclear family and who do not feel threatened by the internet. They include people who use it for business, those who use it for pleasure and those, especially in their 20s and 30s, who use it as a way of social networking.[138]

Other first term measures

In conjunction with its commitment to internet filtering, in the May 2008 Budget the Government allocated $125.8 million over four years to other Internet safety measures. These included cyber safety education, cyber safety awareness-raising activities and law enforcement in areas such as:

- expanding child protection operations in the Australian Federal Police (AFP) to assist it to detect and investigate online child sex exploitation and[139]
- improving the time frame under which the Commonwealth Director of Public Prosecutions was able to manage increased activity resulting from AFP work to ensure that prosecutions proceeded.[140]

The budget measures also included funding for ACMA to:

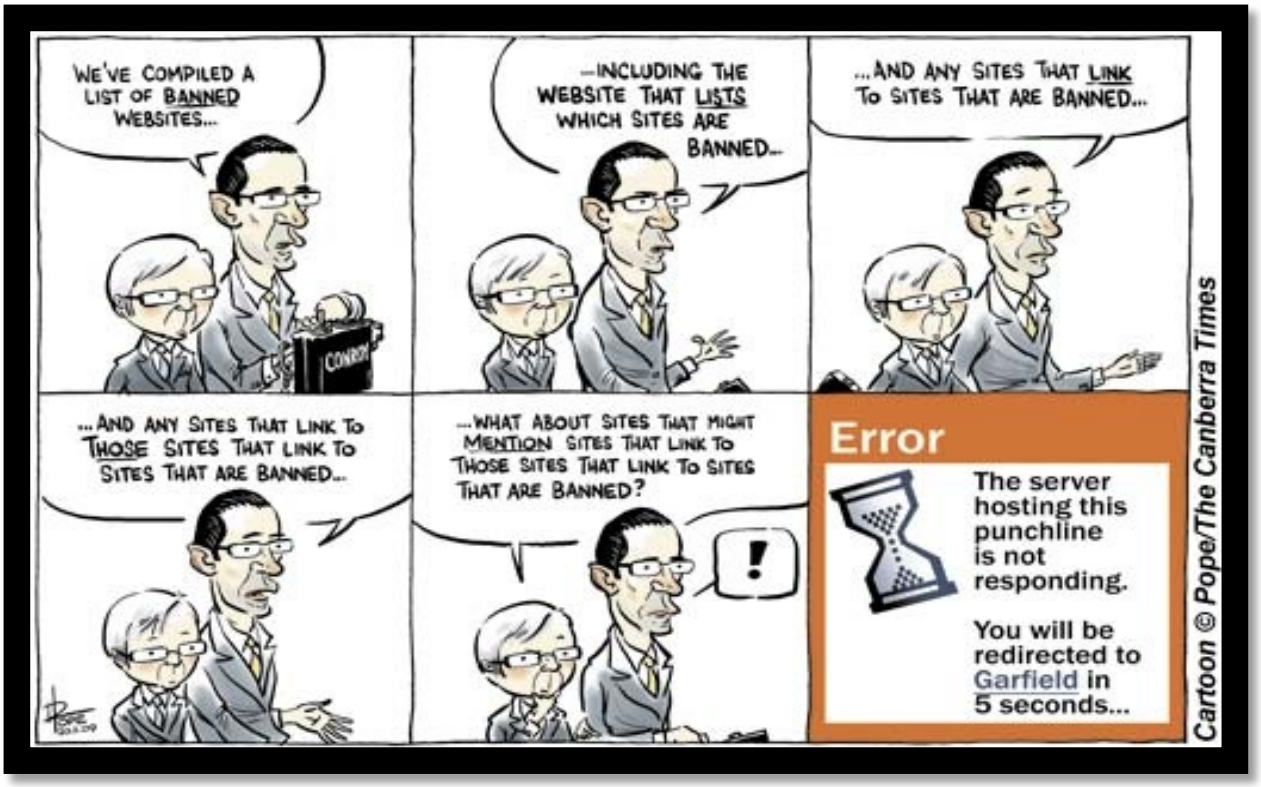
- implement a range of cyber safety education activities, including improving government cyber safety website resources to make them easier to use[141]

---

134. Editorial, 'Filtering threatens freedom but won't stop net nasties', *The Age*, 17 December 2009, p. 22, accessed 28 October 2013.
135. A Moses, 'Hacker raid condemned', *The Age*, 11 February 2010, p. 8, accessed 28 October 2013; and 'Internet protest crashes websites', *Mercury*, 11 February 2010, p. 7, accessed 28 October 2013. Operation Titstorm raised other issues, particularly those relating to cyber terrorism and the question of how the current Australian anti-terrorism law framework applies to politically motivated cyber-attacks. This paper is not able to address this issue, but a worthwhile discussion can be found in K Hardy, Operation Titstorm: hacktivism or cyberterrorism?**'**, *University of New South Wales Law Journal*, 32(20, 2010, pp. 474–502, accessed 12 February 2014.
136. 'Hackers "titstorm" the PM', *The Australian*, 11 February 2010, p. 8, accessed 28 October 2013.
137. Moses, 'Hacker raid condemned', op. cit.
138. R Fitzgerald 'Internet censorship remains part of Conroy's agenda', *Weekend Australian*, 8 May 2010, p. 7, accessed 19 November 2013.
139. More detail on online child protection operations can be found on the Australian Federal Police website, accessed 19 November 2013.
140. Australian Government, Budget measures; budget paper no.2: 2008–09, accessed 12 February 2014.
141. The cyber safety website is Cybersmart, accessed 19 November 2013.

- expand a consultative working group[142]
- form the Youth Advisory Group on Cyber Safety to provide advice to the Online Safety Consultative Working Group on cyber safety issues from a young person's perspective and[143]
- undertake cyber safety research to identify issues and target future policy and funding.[144]

Figure 3: a view of Labor's filtering proposal



Source: *The Canberra Times*[145]

Policy turnaround

The filter on hold

Despite promising to introduce the legislation to implement mandatory internet filtering during its first term, the Labor Government did not do so.[146]

In the lead-up to the 2010 election, while Prime Minister Kevin Rudd continued to express his commitment to the filter, opposition to the idea was beginning to surface in his own party. In late February 2010, Senator Kate Lundy put forward an optional filtering proposal, under which households would be able to indicate to their ISPs if they wanted a filter rather than having one automatically in place.[147] Senator Conroy refused to comment on the alternative proposal, however, and appeared to dismiss continued questioning of the effectiveness of the filter as well as escalating international condemnation from groups such as Reporters Without Borders and the United States' Government.[148]

142. See: Department of Communications (DoC), 'Online Safety Consultative Working Group', DoC website, accessed 30 January 2014.
143. See: DoC, Youth Advisory Group on Cybersafety, DoC website, accessed 30 January 2014.
144. DoC, 'Cyber safety research', DoC website, accessed 30 January 2014.
145. David Pope, Cartoon from *The Canberra Times*, 26 March 2009, as reprinted on Civil Liberties Australia website, accessed 9 October 2013.
146. N Berkovic, 'Rudd retreats on passing web filter legislation', *The Australian*, 29 April 2010, p. 6, accessed 28 October 2013.
147. A Sharp, 'Opposition grows to internet filter', *The Sydney Morning Herald*, 25 February 2010, p. 5, accessed 30 January 2014.
148. P Smith, 'Conroy ignorant of internet filtering dissent', *The Australian Financial Review*, 31 March 2010, p. 58; and A Sharp, 'Censorship fears over Australian net filter', *The Sydney Morning Herald*, 13 March 2010, p. 7, accessed 30 January 2014.

By April 2010 rumours were circulating that the filter had been, at least temporarily, abandoned. Senator Conroy and Prime Minister Rudd denied this was the case, and even after a change of Labor leadership, the new Prime Minister, Julia Gillard, insisted that the filter was necessary to control the 'dark side' of communications technology.[149] Nonetheless, Prime Minister Gillard did not appear to be as committed to the filter as her predecessor and it was soon announced by Minister Conroy that it was 'on hold' for a year, during which its design was to be examined by an independent expert.[150] Conroy later clarified that if the Government was re-elected then legislation to introduce the filter would not be introduced until after a review of classification rules—to be conducted in co-operation with the states and territories—had reported its findings.[151]

One source insisted that Conroy's changed approach was due to the fact that three of Australia's largest ISPs—Telstra, Optus and Primus—had voluntarily agreed to block child pornography web pages on a list maintained by ACMA:[152]

> As soon as Mr Rudd was deposed as prime minister [by Julia Gillard], the filtering laws were postponed. Officially the Gillard government remains committed to the filter legislation, but will take a year to review existing censorship arrangements, which were written well before the borderless world of online communications emerged. In the interim, Senator Conroy has delivered a much better outcome. A deal with Telstra, Optus and Australian members of the Internet Industry Association will result in those organisations voluntarily filtering out child abuse material—the central issue around which the filter debate revolves.
>
> The compromise with industry raises the valid question that if ISPs are willing to filter out abhorrent material using the kind of blacklist that was proposed to underpin legislation, why is cast-iron black-letter law needed? A voluntary agreement achieves essentially the same outcome that mandated measures would have, but without the fuss, cost or additional regulatory burden. Only weeks ago, Senator Conroy delivered an $11 billion compromise with Telstra to get the controversial NBN rolling. The industry solution to internet filtering is a welcome move that should deliver an outcome that black-letter law would have been challenged to produce.[153]

Following Senator Conroy's announcement, the Coalition iterated its promise that if it won government it would abandon any idea of a filter—not only because the idea was flawed, but because it favoured encouraging parents to take more responsibility for their children's web use.[154]

Shifting priorities

It can be argued that Labor's decision to put the idea of filtering the Internet on hold was simply a practical one, given that it faced a Senate in which neither the Coalition nor the Greens supported its filtering plans. It seemed clear, therefore, that, until the composition of the Senate changed in its favour, any legislation it introduced for this purpose was doomed to fail.[155]

The decision may have been more complex, however, for it seemed that the Government sensed a shift in both international and domestic thinking about what constituted, and what was meant by Internet safety.[156] The safety focus appeared in fact to be moving from one which stressed family security to a broader notion represented by the idea of cyber security.[157] It can be argued this is reflected in Labor's 2010 election material,

149. A Sharp, 'Gillard to stick with web filter despite disquiet', *The Sydney Morning Herald*, 8 July 2010, p. 5, accessed 30 January 2014.
150. J Massola, 'Conroy puts net filter on hold for year', *The Canberra Times*, 10 July 2010, p. 5, accessed 9 October 2013.
151. D Harrison, 'Gillard dodges flak over filter', *The Age*, 10 July 2010, p. 1, accessed 30 January 2014.
152. F Foo, 'Telstra and Optus to start "clean feed"', *The Australian*, 10 August 2010, p. 25, accessed 9 October 2013.
153. Editorial, 'Smart compromise on internet filtering, *The Australian Financial Review*, 14 July 2010, accessed 10 February 2014.
154. C Gamble, 'Drawing the line in digital world', *The Canberra Times*, 14 August 2010, accessed 10 February 2014.
155. C Bernardi, 'Second reading speech: Telecommunications Legislation Amendment (Competition and Consumer Safeguards) Bill 2009', Senate, *Debates*, 10 March 2010, p. 1492, accessed 9 October 2013; and S Ludlam, 'Matter of public interest: Internet content', Senate, *Hansard*, 12 May 2010, p. 2604, accessed 9 October 2013.
156. D Ramli, 'Hackers declare cyber war on banks', *The Australian Financial Review*, 22 June 2011, p. 59, accessed 10 October 2013.
157. The definition of cyber security from International Telecommunication Union, the United nations' agency for information and communications technologies Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against

which emphasised cyber and identity security, and in the later interim report by the Joint Select Committee on Cyber-Safety, which was published in June 2011. According to analysis by Ronald Deibert and Rafi Rohozinski for the Open Net Initiative:

> … a sea change has occurred in the policies and practices of Internet controls. States no longer fear pariah status by openly declaring their intent to regulate and control cyberspace. The convenient rubric of terrorism, child pornography, and cyber security has contributed to a growing expectation that states should enforce order in cyberspace, including policing unwanted content. Paradoxically, advanced democratic states within the Organization for Security and Cooperation in Europe (OSCE)—including members of the European Union (EU)—are (perhaps unintentionally) leading the way toward the establishment of a global norm around filtering of political content with the introduction of proposals to censor hate speech and militant Islamic content on the Internet.[158]

Further, the shift in policy direction may also have been linked to possible consequences arising if nations acted on recommendations put forward by the multinational corporation specialising in internet-related services and products, Google, in a white paper issued in November 2010. The Google paper claimed that censorship of the Internet by governments was tantamount to trade war.[159] Consistent with the original premise that the Internet was built and was intended to provide openness and freedom to connect to, and interact with other users, Google argued that to realise the full potential of the Internet as a global marketplace and platform for innovation, policymakers needed to break down barriers to Internet commerce. For Google, one means of doing this would be to take appropriate action if government restrictions on the free flow of online information violated international trade rules.[160]

Shift in focus—internet safety

Labor again formed government following the 2010 election—but it faced a situation where it would need to rely on a number of independent members in order to run its full term.[161] None of these members was supportive of the idea of mandatory filtering of the Internet and all voiced arguments that had previously been raised. The Independent Member for Lyne in New South Wales, Rob Oakeshott, for example, was concerned that the Government's planned filtering had the potential to reduce broadband speeds and Andrew Wilkie, Independent Member for the Tasmanian seat of Denison, believed the proposed internet filtering policy was 'inconsistent with the nature of the Web'.[162] Hence, political reality appeared to have relegated internet filtering, if not to oblivion, certainly to the policy background.

The Government turned therefore to considering alternative ways of looking at, and possibly improving internet safety. One of these was the commissioning of a number of consultations and inquiries which either directly addressed, or obliquely considered safety issues for users of the online environment. Another was to enhance and promote the education and consultative measures it had introduced during its first term.

Inquiries

Joint Select Committee on Cyber-Safety

Of particular relevance within the context of the changing approach to cyber safety was the report of the Joint Select Committee on Cyber-Safety (Cyber-Safety Committee), which was established in March 2010 to inquire

---

relevant security risks in the cyber environment. The general security objectives comprise the following: availability, Integrity, which may include authenticity and non-repudiation and confidentiality.

158. R Deibert and R Rohozinski, 'Introducing next generation information access controls', in OpenNet Initiative (ONI), *ONI access: denied controlled contested*, ONI website accessed 10 October 2013.
159. A MacDonald, 'Threat to trade in 21st century', *The Adelaide Advertiser*, 23 November 2010, p. 38, accessed 10 October 2013.
160. Google, *Enabling trade in the era of information technologies: breaking down barriers to the free flow of information*, n. d., accessed 29 January 2014.
161. D Cronin, 'Gillard's true test begins: promise to get working in new era of minority government', *The Canberra Times*, 8 September 2010, p. 1, accessed 9 October 2013. The minority government was based on the *Agreement for a Better Parliament: Parliamentary Reform*, accessed 5 February 2014.
162. R Gedda, 'NBN liked, ISP filter dogs Labor in election wake', *TechWorld*, 23 August 2010, accessed 6 February 2014.

into 'how young people can be empowered and connect to the Internet, and use new technologies with confidence, knowing that they can use them safely, ethically and with full awareness of risks and benefit'.[163]

The Cyber-Safety Committee report from this inquiry, entitled *High-wire Act: Cyber-safety and the Young,* referred to the issue of mandatory filters, providing further insights into the thinking of those who supported them and the views of those who had misgivings about their effectiveness. But it appeared that the debate had moved on, with the Cyber-Safety Committee making no serious attempt either to dismiss or support the Government's original filtering proposal. It noted instead that since the three major ISPs had volunteered to restrict content, two other providers had joined them and that the Government intended to encourage other Australian ISPs to follow this example.[164]

The Cyber-Safety Committee determined in fact that the solution to cyber safety involved an interlacing of components. On the one hand, young people needed to be able to control their own experiences in the online environment through better education, knowledge and skills. On the other hand, there needed to be enhanced privacy provisions in place for the online environment, and parents/carers and teachers and all those who deal with young people had to become more informed about how to stay safe on the Net. Further:

> The myriad of stakeholders involved in promoting safer online environments require[d] innovative, collaborative solutions. Governments, industry, organisations, schools and parents all play crucial roles but they cannot operate in isolation from each other. Governments can play a leadership role and support the development of resources that are suitable for a diverse citizenry. Industry can ensure the safety of consumers, advance technological solutions and protections, and further drive their corporate social responsibilities. Schools are the key places to encourage young people to improve their own safety and online ethics.
>
> The role that parents play in the cyber-safety education of their children also cannot be understated. Not only does the family play an important educative role, it plays an essential supportive role when young people face cyber-safety risks and dangers. In order to keep the lines of communication open with their children, it is vital that parents can assist their children with cyber-safety and cyber-ethics messages. To make this possible, parents need a strong awareness of the excellent resources available to them.[165]

Classification inquiries

As part of the mooted introduction of ISP filtering, the Minister for Communications made a commitment to consult publicly on the process that leads to Refused Classification (RC) material being placed on the RC content list for the purposes of mandatory ISP filtering and how to review those decisions.[166]

Cyber safety was relevant to public consultations surrounding the introduction of an R18+ classification for computer games. One argument presented against introducing the category was that parents already found it difficult to prevent their children from accessing inappropriate material online.[167]

A Senate investigation into the National Classification Scheme and an Australian Law Reform Commission (ALRC) inquiry into censorship and classification also grappled with the issue of what regulation was necessary to ensure that the basic principles of classification were maintained.[168] The ALRC in particular recommended a new classification scheme which better responded to a convergent media landscape. It proposed platform-neutral regulation and, importantly, a shift in regulatory focus to imposing new obligations on content providers to take reasonable steps to restrict access to adult content and to promote cyber safety, as well as co-regulation, and

163. Joint committee on Cyber-Safety, *High-wire act: cyber-safety and the young: interim report*, House of Representatives, Canberra, 2010, p. 443, accessed 31 January 2014.
164. Ibid., p. 442.
165. Ibid., p. xviii.
166. Department of Broadband, Communications and the Digital Economy, *Outcome of public consultation on measures to increase accountability and transparency for refused classification material*, Commonwealth of Australia, Canberra, 2010, accessed 14 February 2014.
167. Media Standards Australia and Commissioners for Children and Young People and Child Guardians (CCYPCG), cited in Attorney-General's Department, *Final report on the public consultation on the possible introduction of an R18+ classification for computer games*, Commonwealth of Australia, 2010, pp. 20–1, accessed 31 January 2014. The *Classification (Publications, Films and Computer Games) Amendment (R 18+ Computer Games) Act 2012* (Cth) was enacted in June 2012 so that the R 18+ category that applied to films also applies to computer games.
168. Senate Legal and Constitutional Affairs References Committee, *Review of the National Classification Scheme: achieving the right balance*, The Senate, Canberra, June 2011, accessed 31 January 2014.

more industry classification of content and industry development of classification codes, subject to regulatory oversight.[169]

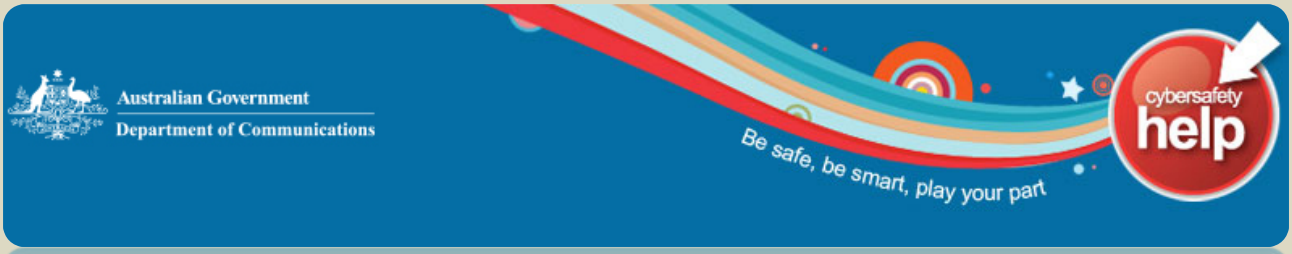
The Government responded to these reports in August 2012, agreeing in principle that the National Classification Scheme should apply equally to all content, regardless of the medium of delivery.

Other initiatives

Minister Conroy introduced a cyber safety help button in December 2010 and in 2012 an easy guide to socialising online was added to the means available to assist people in dealing with Net pitfalls.[170] See Box 9 below for detail on the Cyber Safety Help Button.

Box 9: Cyber Safety Help Button

The Cyber Safety Help Button is a downloadable resource that provides a 'one-stop-shop' for online safety information and advice. The free resource has a talk option so those experiencing cyberbullying or those who have experienced something online that has made them feel uncomfortable can speak with professional counsellors. Users can also report inappropriate content or behaviour to ACMA or the AFP and they can learn about various online safety practices.



Source: Department of Communications[171]

A new era or back to the future?

Mandatory filtering abandoned

In November 2012, the Government officially changed its stance on mandatory filtering when Minister Conroy announced that the Government had abandoned plans for mandatory filtering.[172] Instead, it would require ISPs, under the *Telecommunications Act 1997*, 'to block child abuse websites on the INTERPOL "worst of" child abuse list'.[173] The Government insisted that this change of heart would achieve its aim of protecting children from internet harm: 'blocking the INTERPOL "worst of" list [would] meet community expectations and fulfil the government's commitment to preventing Australian internet users from accessing child abuse material online'.[174]

169. Australian Law Reform Commission (ALRC), *Classification—content regulation and convergent media*, ALRC report, 118, ALRC, Sydney, 2012, pp. 58–9, accessed 28 October 2013.
170. S Conroy (Minister for Broadband, Communications and the Digital Economy), *Help button for Australians online*, media release, 7 December 2010, accessed 7 February 2014. The *Easy guide to socialising online* provides information about the cyber safety features of different sites, including social networking sites, search engines and online games. Users are able to click on logos for sites to learn how to adjust privacy settings, report inappropriate content and find out more about other safety features. Department of Broadband, Communications and the Digital Economy, *The easy guide to socialising online*, accessed 7 February 2014.
171. Department of Broadband, Communications and the Digital Economy, *The Cybersafety Help Button—important facts*, accessed 14 October 2013 and Department of Communications (DoC), *Cybersafety Help Button download page*, DoC website, accessed 14 October 2013.
172. C Milne (Australian Greens Leader), *Press conference*, transcript, ~~Transcript of press conference~~, 9 November 2012, accessed 14 October 2013 ;and M Turnbull, *Conroy backs down in internet filter*, media release, 9 November 2012, accessed 14 October 2013.
173. Section 313 of the *Telecommunications Act 1997* (Cth), accessed 12 February 2014.
174. S Conroy (Minister for Broadband, Communications and the Digital Economy), *Child abuse material blocked online, removing need for legislation*, media release, 9 November 2013, accessed 14 October 2013. See also: INTERPOL, 'Access blocking', INTERPOL website, accessed 7 February 2014.

Telstra and Optus had agreed to block the INTERPOL list in 2010. Under the new plan the AFP was to issue notices to smaller ISPs requiring them to block child abuse websites and work to assist them in meeting their obligations and preventing their services from being used for illegal activities.

Given the anticipated success of the changes made under the *Telecommunications Act*, Senator Conroy asserted that the Government had no need to proceed with mandatory filtering legislation.

It was reported that axing the mandatory internet filtering scheme would achieve savings of $4.5 million over three years.[175]

So internet filtering was dead—or was it?

Coalition glitch

Only days before the 2013 election, reports of the Coalition policy document on online safety for children stated that, if it won government, the Coalition would introduce legislation to force mobile phone operators and ISPs to install filtering services to block adult content.[176] As it was expected the Coalition would form government after the election, this possibility caused a flurry of publicity and led to a swift rebuttal, with Shadow Minister for Communications and Broadband, Malcolm Turnbull, stressing:

> The Coalition has never supported mandatory internet filtering. Indeed, we have a long record of opposing it.
>
> The policy which was issued today was poorly worded and incorrectly indicated that the Coalition supported an 'opt out' system of internet filtering for both mobile and fixed line services. That is not our policy and never has been.
>
> The correct position is that the Coalition will encourage mobile phone and internet service providers to make available software which parents can choose to install on their own devices to protect their children from inappropriate material.[177]

The 'liberal' way of regulating, first introduced by the Howard Government, was to return.

While initially overlooked in the outbreak of concern about the possible return of compulsory filtering, the Coalition's online safety policy included a number of new proposals. These were to establish a Children's E-Safety Commissioner, to consider legislating to create a new cyber bullying offence and to develop rapid takedown mechanisms which would apply to offensive material published on social media networks.

New directions

Children's E-safety Commissioner

Following its election victory, the Abbott Government commissioned the Department of Communications to release an e-safety discussion paper which sought comments on these proposals by 7 March 2014.[178] With regards to the proposed Children's E-safety Commissioner, the paper proposed the Commissioner would have responsibility, among other matters, for:

- implementing the proposed scheme for the rapid removal of material that is harmful to a child from large social media sites
- working with industry to ensure that better options for smartphones and other devices and internet access services are available for parents to protect children from harmful content and

175. 'Unpopular web filter dumped', *The Australian*, 15 May 2013, p. 10, accessed 12 November 2013.
176. Relevant point is on p. 2 of the original edition of *The Coalition's policy to enhance online safety for children*, Coalition policy document, Election 2013, September 2013, accessed 7 February 2014. Revised edition of Coalition policy to enhance online safety for children, Coalition policy document Election 2013, September 2013, accessed 7 February 2014 and J Taylor, 'Australian opposition vows to implement internet filter by default', ZDnet website, 5 September 2013, accessed 14 October 2013 and M Grimson, 'Coalition in embarrassing backtrack on internet filtering policy', *ABC news online*, 6 September 2013, accessed 14 October 2013. l
177. M Turnbull, *The Coalition's policy to enhance online safety for children*, media release, 5 September 2013, accessed 14 October 2013.
178. Department of Communications (DoC), *Enhancing online safety for children: public consultation on key election commitments*, DoC, Canberra, January 2014, accessed 7 February 2014.

- establishing an advice platform with guidelines for parents about the appropriateness of media content.[179]

The discussion paper stated that the Government's intention was 'to have a single organisation which takes the lead in relation to online safety for children, allowing for greater efficiency and addressing duplication and overlap'.[180]

Dealing with the issue of bullying

As a result of its consultation with the industry while in Opposition, the Government concluded there were inadequate remedies available to deal with material intended to bully children using the Internet; that is, to deal with cyber bullying. It cited a number of sources, including academic assessment, that current measures for dealing with online safety concerns were inadequate (see Box 10 below for a brief discussion of cyberbullying).

Box 10: cyber bullying

People, particularly children, can be cyber bullied or harassed through internet services like email, chat rooms, instant messaging, social networks or through websites. Bullying through the use of mobile phone technologies, such as SMS, also amounts to cyber bullying.

The Australian Institute of Criminology attributes the rise of cyber bullying primarily to children's increased access to the Internet and mobile phones.[181]

Cyber bullying includes teasing, spreading online rumours and sending unwanted or threatening messages or defamatory material. The Australian Communications and Media Authority's cyber bullying website explains that cyber bullying 'can involve social, psychological and even, in extreme cases, physical harm. It can cause shame, guilt, fear, withdrawal, loneliness and depression'. It adds that because children and young people are often online 'it can be hard for them to escape cyber bullying. Nasty messages, videos and gossip can spread fast online and are hard to delete. Sometimes the attackers can be anonymous and hard to stop. This can make it harder for adults to see and manage'.[182]

There is currently no national legislation that specifically covers cyberbullying. However, the Commonwealth *Criminal Code Act 1995* may be used to prosecute those who send threatening or harassing messages or images over the internet or via mobile phones. Before persons can be charged under the *Criminal Code Act*, however, they must be deemed by the law to be responsible for their own actions. Those under ten years of age will not be liable for their actions, while those aged between ten and 14 years will only be liable where it can be proven beyond reasonable doubt that they understood that they should not have committed an offence as prescribed under the Criminal Code.[183]

The Government proposed to introduce a scheme to provide an independent and impartial third party to consider 'disagreements between social media sites and individuals on content complaints, where the content relates to a specific child in Australia'.[184] This would be established by legislation to 'help to build the confidence and trust of Australian families in how social media sites deal with their concerns'. Importantly, the scheme would apply to large social media sites as defined in the legislation. The Government sought comment on what criteria should be applied to define such large sites. Similarly, it raised issues such as who should be eligible to complain about online issues and concerns, what form complaints should take, the process that should be involved in handling complaints and penalties and enforcement.

179. Ibid.
180. Ibid.
181. Australian Institute of Criminology, *Cyber bullying: issues for policy makers*, 2007, accessed 11 July 2014.
182. ACMA, Cyberbullying, ACMA website, accessed 11 July 2014.
183. *Criminal Code Act 1995* (Cth), accessed 11 July 2014.
184. Department of Communications, *Enhancing online safety for children*, op. cit.

A further issue addressed in the discussion paper was whether existing Commonwealth legislation adequately covered cyberbullying and whether it would be appropriate to create a new, simplified cyberbullying offence. Three options were provided for comment:

- leaving the existing offence unchanged while introducing education and measures to increase awareness of how it works
- creating a separate cyberbullying offence covering conduct where the victim is a minor (under 18 years), with a lesser maximum penalty, such as a fine and
- creating a separate civil enforcement regime to deal with cyberbullying modelled on a New Zealand approach.[185]

In his assessment of the Government's proposal, however, *Crikey*'s Bernard Keane considered the policy was 'back to the future'. In Keane's view:

> … there's a sinister addition to the policy: this new internet censor would be able to 'request the operator of a site which does not meet the definition of "large social media site" to join the scheme on a voluntary basis — and may disclose publicly any sites which have been requested to comply but do not'. Thus, even if you're not caught by the legislated remit of the scheme, the censor might try to name and shame you if you don't behave like you are.
>
> The Coalition also proposes to create 'a new, simplified cyber-bullying offence' while freely admitting there's no need to do so because it's already covered under existing legislation relating to carriage services.[186]

It was reported also that the large Internet companies of Google, Facebook and Yahoo!, among others were concerned that the Coalition proposals imposed on them an unworkable regulatory burden.[187] EFA, on the other hand, was concerned about 'the potential for overreach and vagueness of some of the standards proposed' and 'who may end up making decisions', but prepared to wait to see what the Government's final policy involved.[188]

Despite these concerns, and an acknowledgement that it did not have all the answers to dealing with internet threats on the Internet, the Government was determined to proceed with its new approach to cyber safety. In the May 2014 Budget, it allocated $2.4 million to establish the Office of the Children's E-Safety Commissioner and $100,000 to support Australian-based research and information campaigns on information safety. It intends that the Children's e-Safety Commissioner legislation will be before the Parliament later in 2014.

Concluding comments

Perhaps Bernard Keane was a little harsh in his statement that the Government's policy amounted to 'back to the future'. There is, in reality, no 'going back' for the Government; the issue is more about addressing debates and issues that have been a constant with regards to filtering the Internet. As this paper has illustrated, Australian Governments, regardless of who has been in power, have not appeared to dispute that the Internet is a remarkable information and communications tool; all Australian Governments appear to have conceded also that people should be free to use that tool in many and different ways. At the same time, Australian Governments have expressed concern about traps and pitfalls existing for those accessing the Internet, not only for those least able to defend themselves, but also for users of the Internet in general.

What Australian Governments have disagreed about is how to deal with those traps and pitfalls.

There are those who see a very limited role for government in regulating the Net, while others favour more intervention. The Howard Government arguably adopted the most minimalist approach within an ideological

185. As proposed in the Harmful Digital Communications Bill 2013 (NZ), accessed 7 February 2014. The New Zealand Bill provides for a civil enforcement regime under which a person who complains he/she has been the he subject of harmful digital communication may complain to an 'Approved Agency' (it is suggested the Children's e-Safety Commissioner could perform this role in Australia) which can receive and assess complaints, use negotiation, mediation and persuasion (as appropriate) to resolve complaints and investigate complaints. If the matter cannot be satisfactorily resolved through these means, the complainant can go to court and seek various orders including to take down the material.

186. B Keane, 'Back to the future with the Coalition's new Net Nanny policy', *Crikey*, 10 September 2013, accessed 11 February 2014.

187. J Hutchinson, 'Battle looms over e-safety plan', *The Australian Financial Review'*, 21 January 2014, p. 8, accessed 11 February 2014.

188. S Rintel, 'First reaction: discussion paper on enhancing online safety for children', Electronic Frontiers Australia website, 23 January 2014, accessed 12 February 2014.

framework of self-regulation, while adding a touch of government supervision. Yet the Howard Government was criticised by some for doing too much, and for not doing enough by others.

Labor under Kevin Rudd and Julia Gillard was accused of attempting wholesale repression of information availability on the Internet, but its proposals, overseen by Minister Stephen Conroy, were hardly akin to those imposed in regimes such as China and Iran. And it was unlikely that they could have ever been so, given the traditions of democracy that are firmly entrenched in Australia. Indeed, it was the case that because of those traditions, people were free to lampoon and criticise the Minister and his filtering proposals.

Similarly, familiar criticism has surfaced in relation to the current Government's proposals and it is likely that more will emerge when it introduces legislation to deal with internet bullying and to establish the Children's E-safety Commissioner.

What remains constant is that there are predators ready to take advantage of those accessing the Net and the Australian Government has been called upon by some to prevent them from harming Australian citizens—particularly children. No reasonable person disputes this aim, but many dispute the means taken to achieve it. As noted in the introduction to this paper, the governments of western democracies like Australia have, since the 1990s, been confronted by this dilemma—trying to balance the freedoms that come with the Net with the responsibilities they have to protect people from its potential to be used as a means to do harm.