www.aussiefirewall.com.au/blocked

Mitchell Landrigan and Marissa Wong discuss the importance of freedom of expression and the Federal Government's proposed ISP level filtering scheme.

Introduction

We review the Australian government's mandatory ISP filtering regime in this article. Coming from the perspective that free speech is an important measure of the health of a democracy and that the internet can empower people by allowing people to express themselves, we describe some of the benefits of free speech – including that free speech confers upon a person's listeners the fruits of their free expression. Freedom of speech can be socially beneficial, not just individually empowering.

We also believe that the vast majority of people accept that there must be reasonable limits on free expression and that free speech should not be a licence for people to view, download or disseminate images of children in sexually compromising positions. In this sense, we commend the government for its action in seeking to regulate the distribution of such content.

The effectiveness of the mandatory ISP filtering regime is another matter, however. We are unashamedly sceptical about the effectiveness of the regime, believing that, for the most part, it is likely to under-block relevant restricted content (**RC**). We set out our reasoning in more detail when describing the technical limitations of the mandatory ISP filtering regime. However, we recognise that there are inherent limitations in the effectiveness of any ISP filtering regime given the various technical means for accessing internet content.

We note that Senator Conroy, the Minister for Broadband, Communications and the Digital Economy (**Minister**) claims that the Australian government would not seek to block political content when introducing the mandatory ISP filtering regime. We express doubt about how bureaucrats administering the regime would identify political content and raise concerns about the government viewing Australians' free speech protections through such a confined legal prism.

Internet and Free Expression

The importance of free expression

The ability to say something, to express one's view; the capacity to influence others through communication can be vital to a person's self-worth. Perhaps most importantly, free speech can liberate people from the "forgotten freedom", freedom from fear,[1] by allowing people to speak up; and to have a voice against their oppressors, or those who would otherwise put them in harm's way.

The freedom to speak against coercive acts of government is perhaps most important of all freedoms. To some extent, freedom of speech is at the heart of democracy. It is fundamental to the accountability of a government to its citizens, including via the so-called "Fourth Estate" of journalism as a watchdog for the public interest.

Yet equally importantly, when backed by strong and clear legal protections, individuals have the confidence to express themselves – not only about their own views, or those of like-minded individuals, but about the views of those who disagree with them. In short, free speech protections can give people confidence. In expression, doubt breeds doubt and confidence encourages courage.

Contributing to debate – speaking out - brings richer meaning to the speaker's life, both by allowing the person to express themselves and by the listener providing a considered response. Dialogue backed by freedom, can thereby foster learning and intellectual growth. Conversely, frustrating a person's capacities for self expression can be depersonalising; and may stunt the development of people's moral and intellectual competencies.[2]

We are unashamedly sceptical about the effectiveness of the mandatory ISP filtering regime

It is implicit in this reasoning that, where people are able to express themselves, others gain from such freedoms. This is not to say that every speaker is a master orator, or that the person who tends to bloviate is anything other than a loud bore. Yet, allowing people to express beliefs and giving them the confidence to do so, can empower others to express their own beliefs - in short, freedom of expression confers upon an audience the benefits of the speaker's freedoms.[3]

Allowing people to contribute to the society's pool of ideas can also promote a better understanding of truth and a deeper appreciation of what is valuable and worthwhile. Giving people the confidence to speak out about or even distribute what palpably is not beautiful may foster a better understanding of what is not meritorious; or about what is indeed socially harmful. Speech – the communication of beliefs and ideas – can crystallise understanding, shed new perspectives on values and can benefit society's ascertainment of truth, not only about what is beautiful, but about what is immoral and distasteful.

For those with access to it, the internet undoubtedly expands people's scope for self-expression. The socially inept social communicator can find themselves with many followers on Twitter; the never-published letter writer can create an interesting blog; the once-silenced religious critic can compile a website devoted to atheism; and the skilful though shy guitarist can become an overnight hit on YouTube. With relatively few (if any) editorial constraints, the aspiring autobiographer is liberated from editors' rules; and the never-quite-published author can place themselves before an audience of thousands, even millions, without so much as a single peer review. As with expression more generally, speech on the internet can be empowering for the speaker and benefit those to whom speech and content is conveyed.

The internet also has the power to engage and connect people, and to even facilitate political and social movements domestically

---

1 See Hon James Spigelman AC, "The Forgotten Freedom: Freedom From Fear", speech to University of Sydney Law School, Banco Court Sydney 17 November 2009, available at http://www.lawlink.nsw.gov.au/lawlink/Supreme_Court/ll_sc.nsf/vwFiles/spigelman181109.pdf/$file/spigelman181109.pdf, website accessed 23 November 2010.

2 See Michael Chesterman (2000), Freedom of speech in Australian Law – a delicate plant, Ashgate, Sydney, p.302.

3 See Michael Chesterman (2000), Freedom of speech in Australian Law – a delicate plant, Ashgate, Sydney, p.302.

and throughout the world. The power of online communities is perhaps no better illustrated by the proliferation of Web 2.0, or social networking technologies such as Facebook and Twitter. These are tools for building networks[4] – a structure not easily controlled by a single central authority given content on networks can be swiftly created and restored; and achieving "21st century statecraft" – to help individuals be empowered for their own development, and "advance democracy and human rights, to fight climate change and epidemics…"[5]

The internet is a network not a broadcast medium. Its architecture does not readily accommodate the existing censorship controls in the offline world.

Censoring Content on the Internet

Part of the internet's power is the immediacy with which material can be communicated to large numbers of people, anywhere on the planet, in real time. Material on the internet can move, evolve and re-emerge instantaneously and seamlessly. Take, for example, the whistle-blowing website WikiLeaks[6] – a small independent organisation sourcing its material from anonymous individuals. In the week following the release of the secret "Collateral Murder"[7] video showing civilians and journalists being killed by the US army during the Iraq War, "WikiLeaks" was the search term with the most significant growth worldwide as measured by Google Insights,[8] being viewed more than 6.5 million times on YouTube.[9] Despite efforts to contain the video (the US had been refusing Freedom of Information requests for the video for three years), a tiny organisation supported by a handful of volunteers reporting on material sourced from anonymous individuals managed to broadcast globally a secret video, elevate an influential journalist, advance a political message and spark an international uproar.

The internet, however, can also be a vehicle for the uploading of and dissemination of abhorrent material - denigrating pornographic images, urges to violence and war, racist incitements etc. For those willing to search, there is virtually no end to the available range of degenerate content. However, people may hold legitimately different opinions about the appropriateness of online material. Often, matters of degree, taste and individual perception are involved. What is degeneracy for one person is for another harmless fantasy; instructions on voluntary euthanasia may be an informative research source for a student of palliative care, and, for another, an immoral implicit incitement to assisted suicide.

With widely acknowledged artistic merit, the Australian photographer Bill Henson's exhibits in 2008 provide a striking example of how content involving teenage girls can spark wide disagreement about the appropriateness of displaying such content when there are no hard and fast moral norms. The controversy is no less significant for any censorship regime, including that of ISP filtering, than for the professional reputation of the artist himself.[10] For material at the margins of good taste, it is difficult to apply any rule, least of all one of censorship, about people viewing such content.

Further, unlike traditional media, the internet is everywhere – and therein lies its beauty and its weakness. The internet is a network not a broadcast medium. Its architecture does not readily accommodate the existing censorship controls in the offline world. Although traditional media are changing, there is generally a fixed, centralised process for the creation, distribution, importation and exhibition of television, film, radio and print publications. To illustrate, consider the decision to place the pro-euthanasia book The Peaceful Pill Handbook by Dr Nitschke[11] on a banned list – copies of the book were taken off shelves and could not be displayed, sold, distributed or imported into Australia. The publication was effectively restricted as there were identifiable points of control. Further, it was well known that the book was censored and the decision generated a healthy debate about the merits of the ban by the Office of Film and Literature Classification (**OFLC**).

By contrast, if we consider access controls when applied to the internet, access controls do not have the same effectiveness, because one cannot easily identify: a) the identity of the content producer and receiver; b) the jurisdiction of the content producer and receiver; or c) the content at issue, particularly in cyberspace where content has a habit of propagating and reappearing in mul-

4 Despite recent concerted attempts by the Iranian government to block news and images about the re-election of President Mahmoud Ahmadinejad, ordinary Iranians, via Twitter (and now dubbed as "Twitter Revolution"), were able to deliver information from street level, in real time. Protestors, activists and dissidents were able to connect and communicate scarce information and organise a mass political movement. The Iranian government engaged in both news media censorship and Internet censorship. Journalists were barred from reporting, news broadcast feeds into the country were jammed, access to Facebook, Twitter, and other social networking sites were blocked and on 13 June as the election results were being announced, Iran shut down all Internet access for about 45 minutes.

5 In a series of speeches, the Secretary of State Hillary Clinton launched the "21st Century Statecraft" initiative – a program to encourage diplomatic efforts not just from one government to another, but from government to people, people to government, and people to people. See: http://www.state.gov/statecraft/index.htm, website accessed 2 December 2010.

6 http://www.wikileaks.org. On 16 March 2009, the ACMA added WikiLeaks to the proposed blacklist of sites that will be blocked for all Australians.

7 On 5 April 2010, WikiLeaks released classified U.S. military footage from a series of attacks on 12 July 2007 in Baghdad by a U.S. helicopter that killed 12, including two Reuters news staff, Saeed Chmagh and Namir Noor-Eldeen, on a website called "Collateral Murder".

8 http://www.independent.co.uk/news/media/current-google-insights-trends-wikileaks-posts-clasified-military-video-masters-1942629.html, website accessed 28 November 2010.

9 http://blog.thoughtpick.com/2010/05/power-of-annonymous-wikileaks.html, website accessed 28 November 2010.

10 The opening night of Henson's exhibition at a Sydney gallery was cancelled after police received a number of complaints about an email invitation to the exhibition that included images of a nude 13 year old girl. Police later removed photographs from the gallery and considered charging Henson with publishing indecent material under the Crimes Act 1900 (NSW). Claiming the images had no artistic merit (though without having seen them), the then Prime Minister Kevin Rudd described the images as "absolutely revolting". The Classification Board later assessed the online reproduction of six of the Henson works, finding one "mild and justified" and PG-rated, and the others "very mild", or G-rated. In the end, perhaps unsurprisingly, the police did not charge Henson. See Matthew Westwood, PM says Henson photos have no artistic merit, 23 May 2008, http://www.theaustralian.com.au/news/nation/nude-teen-exhibit-not-art-rudd/story-e6frg6nf-1111116421927, website accessed 22 November 2010; AAP, Rudd stands by criticism of Henson images 28 May 2008, http://www.theage.com.au/news/national/henson-still-revolting-pm/2008/05/28/1211654079734.html, website accessed 22 November 2010; and . Andrew Drummond, Ninemsn, 7 June 2008, http://news.ninemsn.com.au/article.aspx?id=575939&rss=yes, website accessed 22 November 2010.

11 Philip Nitschke & Fiona Stewart (2006), Peaceful Pill Handbook, Exit International US. The book had previously been classified Category 1 Restricted (meaning it could only lawfully be sold to adults over the age of 18 and in a sealed plastic wrapping) in 2006 by the OFLC. Following an appeal by the NSW Right to Life Association and then Federal Attorney-General, Philip Ruddock, the OFLC upgraded the rating in 2007 to Refused Classification, making any print editions of the book banned from sale in Australia.

tiple locations. Additionally, content in cyberspace is broken into packets (and sometimes is encrypted), and not all packets will necessarily pass through the same channels.

Once we appreciate the dynamic nature of the internet, we start to realise the difficulty with applying access controls to censor it.

Returning to Peaceful Pill Handbook, online electronic versions of the book are now available from a variety of sources for people to view, purchase and download in full, including, just to name a few: Dr Nitschke's own website;[12] Amazon.com, Google Books; YouTube; and peer-to-peer networks. The material in the book is also available online in various digital forms (e.g. videos, images, sound bites, excerpts from the book), not to mention the fact that people could freely discuss and critique on chat rooms and email. Once we appreciate the dynamic nature of the internet, we start to realise the difficulty with applying access controls to censor it.

The mandatory ISP filtering policy and free expression

Australia is alone amongst Western democracies in that ordinary discourse (artistic expression, music, dance, theatre, ballet, media commentary and enunciation of unpopular, contentious or impolitic views) comes with no explicitly recognised legal free speech protection (as would exist in a Bill of Rights or Charter).[13] The implied freedom protects political speech, but there is otherwise no undergirding Constitutional protection for the writings of journalists, programs of broadcasters, commentators' opinions, the writings of academics or the scripts and screenplays of playwrights. Least of all is there any transparent free speech protection for blogs, tweets, YouTube clips, emails, or content on peer-to-peer files.

Freedom of speech in Australia, including on the internet, is, as one writer describes it, a delicate plant.[14]

The government's ISP filtering regime's RC list will comprise a list of websites that are the subject of a complaint to Australian Communications and Media Authority (**ACMA**) and are either classified as RC content by the Board or are assessed to be RC content by trained officers within ACMA applying the guidelines of the National Classification Scheme. Alternatively, RC material can be included on the list via arrangements with 'highly credible overseas agencies'.[15]

In a speech on the ISP filtering regime, the Minister said that, as:

> [f]reedom of speech is fundamentally important in a democratic society, the Australian government would [not] seek to block political content [when introducing internet filtering]. [16]

Doubtless conscious that the ISP filtering regime must not infringe the implied freedom of political discourse, three things may be said about Senator Conroy's defence of the regime in relation to free speech.

First, it is unclear how bureaucrats administering the RC list would determine whether content is political – what is one person's political concern may be another person's irrelevance. For example, a budding documentary director may consider graphic footage of young teenagers having unprotected sex to be a political matter (about, say, the adequacy of the government's health funding for sufferers of AIDS), but, for those administering the ISP regime and potentially blocking the content, the film may represent licentiousness and gratuitous nudity.

Secondly, by its nature, political content changes from time to time: what is political one day may not be political on another. How, and according to what principles, would the government unblock censored content if content becomes political - and what would the process be (and how long would it take) to correct any unintended filtering of political content? How much damage could be done to Australia's democratic process if the mandatory ISP filter were to systematically over-block political content? Answering these questions is not made easier by the fact that the government has been quite ambiguous about the intended scope of the targeted material and even when there is consensus on what content should be filtered, blocking tends to restrict both too much and too little content. [17]

There is nothing particular particularly remarkable about censorship or limits on free speech.

Thirdly, if the reader will forgive a double-negative, the Minister offered no comfort that internet filtering would seek to protect non-political expression. To put the point more directly, Senator Conroy seems not to recognise any more general freedom of expression Australians might want to enjoy to, say, produce, view or download apolitical comedic, music, or artistic content. While we recognise that Australians' freedoms of expression only includes political discourse in a Constitutional legal sense, the Minister's speech is a stark reminder of the comparative narrowness of Australia's legal free speech protections in relation to other Western democracies.

The government's ISP filtering policy

The government's mandatory ISP filtering regime is a censorship regime. It constrains free speech ostensibly in the public interest. There is nothing particular particularly remarkable about censorship or limits on free speech. We often take censorship for granted. While on an aircraft, a passenger is not entitled to falsely shout "there is a bomb on board"; nor is the moviegoer allowed to lie and shout "fire" to the distress and panic of others in a cinema; for the most part, and absent any particular redeeming literary qualities, governments should probably ban most books that promote bomb-making. People are entitled not to be subjected to unnecessary terror and likewise should be protected from defamation and vilification (other legal constraints on free expression).

---

12 http://www.peacefulpillhandbook.com. In May 2009, WikiLeaks revealed that this website was include d on the ACMA blacklist.

13 While the High Court of Australia recognises an implied freedom of political discourse under the Constitution, this freedom acts a restraint of legislation that serves to stifles political expression (and applies when the legislation is not reasonable and adapted to its intended purpose); the implied freedom confers no rights of free speech. For a discussion of the application of the implied freedom to internet filtering, see Chris Govey (2010), Won't Somebody Please Think of the Children: Would a Mandatory ISP-level Filter of Internet Content Raise Freedom of Communication Issues?, Communications Law Bulletin Vol 28 No 4, p.14 at 15.

14 See generally Michael Chesterman (2000), Freedom of speech in Australian Law – a delicate plant, Ashgate, Sydney. Australia's Constitution provides no general right for people to free expression.

15 Chris Govey (2010), Won't Somebody Please Think of the Children: Would a Mandatory ISP-level Filter of Internet Content Raise Freedom of Communication Issues?, Communications Law Bulletin Vol 28 No 4, p.14 at 15.

16 See Senator Stephen Conroy 20 January 2009, Address to ALIA Information Online Conference and Exhibition, available at http://www.minister.dbcde.gov.au/media/speeches/2009/001, website accessed 24 November 2010. Emphasis added.

17 See Derek E. Bambauer, Filtering in Oz: Australia's Foray into Internet Censorship, 31 U.Pa.J.Int'l L. 493 2009-2010, p.508

It is appropriate for democratic governments (including Australia's) to prohibit the distribution of some content

Democratic societies also recognise that there should be limits on the accessing, downloading and dissemination of socially harmful material, including child pornography, and free expression ought not to be a license for viewing or distributing such material.

We believe that the Australian government is right to be concerned about the social harm that can arise from the exploitation of innocents for others' sexual gratification – the concern which seems to be at the heart of the government's mandatory ISP filtering regime.[18] Most Australians rightly regard content about such matters as so offensive and repugnant to ordinary good taste (not to mention harmful) that there should be no freedom to publish, disseminate or download such material at all. The majority of reasonable people also rightly see as indefensible the suggestion that distributing images of children in compromising (or even suggestive) sexual positions is a legitimate form of self expression. It is appropriate for democratic governments (including Australia's) to prohibit the distribution of some content – including, for example, sexually explicit images of children.

This is not to say that the Australian government's ISP filtering regime is likely to be effective. It is simply to say that the government is well-intentioned. For a variety of reasons soon to be explained, we doubt that the government's ISP filtering regime is likely to be any more effective in limiting the distribution of harmful content than it would be for police to drape arrest nets around randomly chosen houses in the hope of catching fleeing criminals.

Technical Limitations of the government's ISP filtering regime

Internet and the World Wide Web

The World Wide Web (**WWW**) is only one part of the greater internet, which is made up of various online transmissions and protocols including peer-to-peer systems (e.g. BitTorrent), newsgroups, Internet Relay Chat (IRC), email, file transfer protocols, internet telephone, Virtual Private Networks, chat rooms, internet messaging services, etc. The government's proposed ISP filtering of a blacklist of RC websites would only be performed on the WWW (HTTP). This does not address the vast information stores and content distribution channels which act as a natural domain for truly offensive material, including via internet chat rooms, peer to peer, file transfer protocol and email.[19]

Sophisticated offenders are more likely than most to use anonymous technologies. It follows that just concentrating on censoring the WWW will not catch illegal material disseminated through covert and often encrypted channels. Nor will doing so address the underlying concern about distributing pornographic content or significantly affect those who deliberately produce, distribute or go in search of illegal material.

Efficacy of the ISP filtering regime

Recognising that the characteristics and peculiarities of the internet make it inherently difficult to censor online content, we now consider the likely efficacy of the government's ISP filter regime. One key limitation of the government's policy is that it seeks to retrofit mandatory ISP filtering to a network infrastructure that did not envisage such a need as a design goal.[20] More specifically, it is possible for filtering to occur at different points within the network architecture: on the centralised backbone of the internet infrastructure; at the decentralised ISP level; at the institutional level (companies, government, schools etc); and at the individual computer level. The filtering regime will require ISPs to block specific web page addresses on the ACMA blacklist.[21] Although the intuitively obvious place to locate the filter would be a centralised control point in the backbone service provider at the international gateways, Australia's decentralised network infrastructure means that ISPs must necessarily be involved given their direct relationship with the international gateways.[22]

it is possible for filtering to occur at different points within the network architecture

There are several implementation limitations with this kind of ISP-based uniform resource locator (**URL**) filtering including the administrative overheads involved in compiling a large and accurate list of content deemed prohibited. To implement the regime would appear to require a large team of trained bureaucrats just to oversee the continued accuracy of the list.

Other limitations of the ISP filtering regime include (but are not confined to) the following. First, it will be difficult for the scheme to keep pace with the amount of new content published on the web.[23] Secondly, URLs can easily be renamed; once this occurs, the relevant URL address will no longer match the address on the blacklist. Given the Minister has indicated the ISP filtering regime will apply to web pages, this would appear to be a critical limitation of the regime. In addition, many websites have mirrors and multiple URLs and if the blacklist were to not include all the relevant URLs, then the filtering process would be ineffective. Thirdly,

---

18 Senator Conroy has stated that "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": see Senator Conroy (2007), Labor's Plan for Cyber Safety, available at http://stilgherrian.com/wp-content/uploads/2010/06/labors_plan_for_cyber_safety.pdf, website accessed 2 December 2010..

19 See for example, Australia Computer Society, "Technical Observations On ISP Based Filtering Of The Internet", Oct 2009: https://www.acs.org.au/attachments/2009/ispfilteringoct09.pdf, website accessed 2 December 2010.

20 See Derek E. Bambauer, Filtering in Oz: Australia's Foray into Internet Censorship, 31 U.Pa.J.Int'l L. 493 2009-2010, p.508.

21 Senator Conroy announced on 15 December 2009 the third version of Labor's mandatory blocking plan. In his media release (available: http://www.minister.dbcde.gov.au/media/media_releases/2009/115, website accessed 28 November 2010), he stated that the "Government will introduce legislative amendments to the Broadcasting Services Act to require all ISPs to block [Refused Classification] RC-rated material hosted on overseas servers.". In an interview two days later (available: http://www.zdnet.com.au/conroy-explains-his-magic-filter-339300104.htm, website accessed 28 November 2010) , Senator Conroy further clarified that the URLs required to blocked will be those of specific Web pages, not entire Web sites ... "we are only blocking specific web pages, not web sites, so we get a specific URL address and we target the specific URL address."

22 Australia's decentralised model can be contrasted with the centralised system of Internet filtering in Iran and China where Internet traffic is filtered at discreet control points.

23 ACMA's blacklist contained 1421 URLs as at April 30 2010, with 54 per cent categorised as RC.

the mandatory ISP filtering regime appears to be only at best a partial solution to the underlying issue

push technologies (such as RSS) allow for the sending of content directly to the user, thereby evading an ISP filter. Fourthly, and most obviously, not all users access the internet using an ISP[24] in which case the filter won't work at all.

There are also many methods to circumvent ISP-based URL filtering. A first method, mirroring, is where users may access a blocked site through a duplicate (or mirror) website.[25] This requires users to know the URL or the IP address of the mirror; i.e., a replica website with the same content available at different IP addresses and different computer servers. For example, Wikipedia is mirrored at numerous locations including Reference.com, Answers.com and Wapedia.com. A second method of circumventing the filter is via additional domain names. Websites often have several domain names pointing to the same IP address where blocked content may reside. For example: www.yahoo.net and www.yahoo.org both direct users to www.yahoo.com. Thirdly, using anonymisers, users can configure their web browsers to seek content through a proxy server (an anonymiser) to gain access to sites rather than directly accessing the site. ISP filtering software will see only the URL of the anonymiser and will not recognise the URL of the site being requested. A fourth means of circumventing ISP filtering is via translators and encryptors. These sites translate web page text into different languages or encrypt text. Typically a user will enter the URL of the website to be translated or encrypted and translation software will present the translated information within its own web page thereby hiding the URL of the blocked site from the ISP filtering software. A fifth method of circumvention is via alternative network paths. Comprising client software and a network of servers which can hide information about users' locations and other factors which might identify them, services such as TOR, also known as Onion Router, enhances bypass traditional internet traffic analysis. Sixthly and more generally, it is possible to bypass ISP filters using encryption protocol (for example Reset packets are used with BitTorent traffic to avoid blocking) and secure networks (like Virtual Private Networks). Finally, material abounds on the internet to guide users on how to bypass both sophisticated filtering systems[26] such as those in China and Iran (including proxy servers, language translation services) and ISP level blocking.[27]

Given the Australian government's mandatory internet filtering regime focuses on blocking specific websites (or URL addresses), we believe it can really only reduce accidental or inadvertent access and therefore suffers the risks of under-blocking. In short, therefore: the effectiveness of the filter is questionable (the filter itself can be easily bypassed or circumvented); and ISP-level filtering systems and products are not capable of reducing the risk of access to material that is available via non-web internet technologies. As such, the mandatory ISP filtering regime appears to be only at best a partial solution to the underlying issue.

The question arises whether the implementation of a partial solution has net benefits for Australian society relative to no solution at all. The nature of the internet may mean that a complete solution to this problem is largely impossible without implementing a country-wide firewall in the nature of that imposed by the Chinese government on its population. Yet such a country-wide firewall would appear to give the government significant discretionary power that is open to political abuse. Bearing in mind the important caveats in this article, we suggest that the proposed partial solution may be appropriate but should be applied with caution.

Bearing in mind the important caveats in this article, we suggest that the proposed partial solution may be appropriate but should be applied with caution.

Conclusion

In this article, our aim has been to explain why free speech is important in a democracy like Australia. While acknowledging that there must be reasonable constraints on free expression and although we support the government's desire to limit the distribution of socially harmful content (particularly child pornography), we have doubts about the effectiveness of the mandatory ISP filtering regime. Specifically, we believe the regime is likely to under-block RC, although some blocking is an improvement on no blocking of RC. Equally importantly, while the Minister has (helpfully) recognised Australians' freedom of speech, we doubt that the government could ever realistically guarantee to not block political content under the mandatory ISP filtering regime. It is the risk that such ISP filtering could be used to block legitimate content that is the real concern, including material, such as WikiLeaks, which may be important to government accountability.

Mitchell Landrigan and Marissa Wong are both Legal Counsel at Telstra Corporation Limited and Mitchell is a Visiting Fellow, Faculty of Law, University of Technology Sydney. The authors wrote this article in a personal capacity. The views expressed in the article are the authors' and do not reflect the views of Telstra Corporation Limited or any other organisation or individual. ***The authors thank Dr Martyn Taylor, Partner, Gilbert & Tobin for his helpful comments on an earlier draft.*** ***The authors can be contacted at, respectively, mitchell.landrigan@gmail.com and marissa.wong@gmail.com.***

---

24 We also note that in the trial ISP filtering pilot for the Australian regime, there was some effect on performance (that is upload/download speed) during the performance degradation tests, although this impact was generally within the stated +/ 10 percent margin for error. One of the four ISPs involved in the testing, using a particular technical setup, experienced a 'noticeable' (> 20 per cent) impact on file uploads and a 'minimal' (10 per cent to 20 per cent) impact on file downloads when filtering the ACMA blacklist only. Significantly more performance degradation was evident for all ISPs when the ACMA blacklist as well as additional content was filtered.

25 Duplicate websites are used to reduce the traffic load on servers hosting high traffic web sites.

26 For example The Citizen Lab, University of Toronto, "Everyone's Guide to By-Passing Internet Censorship" September 2007, available at: http://www.nartv.org/mirror/circ_guide.pdf, website accessed 28 November 2010. This guide is intended for the non-technical user and provides tips and strategies on how to by-pass content filters worldwide.

27 For example, Reporters sans frontières/Reporters Without Borders, "Handbook for bloggers and cyber-dissidents. – Technical ways to get around censorship", 12 March 2008 , available at: http://www.rsf.org/IMG/pdf/handbook_bloggers_cyberdissidents-GB.pdf?PHPSESSID=7e180fabc21e4000499fb2e8b24273a2, website accessed 28 November 2010 and Adam Turner, Sydney Morning Herald 'Gadgets on the Go' Blog, "How to easily bypass Australia's internet filters for free", 3 November 2008, available at: http://blogs.smh.com.au/gadgetsonthego/archives/2008/11/how_to_easily_bypass_australia.html, website accessed 28 November 2010