THE GREAT FIREWALL OF AUSTRALIA

Mandatory internet filtering has economic and political risks, argues **Chris Williams-Wynn**

Despite strong opposition, the federal government continues to support mandatory filtering of the internet, seeking to establish a 'Great Firewall of Australia.' If filtering is implemented, all internet service providers (ISPs) would have to scan their internet traffic in real time, blocking access to sites that appear on a government blacklist. Both domestic and international traffic would be subject to this scanning procedure. Filtering would significantly extend existing internet censorship, which requires Australian sites with material contravening Australian law to be taken offline, but which cannot effectively deal with overseas content.

Web pages containing material that has been or would receive a 'Refused Classification' (RC) rating would be blacklisted. RC ratings are given to material depicting child sex abuse, bestiality, sexual violence, and detailed instruction of crime or drug use. Though the government's public statements on filtering have focused on reducing the exposure of minors to illicit material, filtering would affect a much wider range of materials.[1] The government will also encourage ISPs to offer additional filtering services that block more content as requested by users such as families. This could block X, R and M rated web pages. While protecting children is an admirable goal, pervasive ISP filtering creates real economic and political concerns that the government has failed to address.

Economic concerns

Given the importance and ubiquity of the internet in today's world, any reduction in performance will come at great cost to businesses both large and small. Research published by the Australian Communications and Media Authority (ACMA) in 2008 highlights the potential costs associated with ISP-level filtering.[2] Five of the six products tested resulted in performance degradation of at least 22%. The results of the government's 2009 ISP Filtering Live Pilot, conducted by Enex Testlab, found that filters had a 'negligible impact' on performance for ISPs in the test, meaning speeds could drop by 10%.[3] However, this statistic refers to filtering of content on the ACMA blacklist. When filtering additional material, speeds for some ISPs dropped by more than 20%. Furthermore, these filtering tests were performed at a high-speed data centre in Melbourne, suggesting actual performance degradation for typical users may be even higher.

'Over-blocking,' the filtering of content that should not be blocked, is another potential problem. The 2008 ACMA paper reported that up to 8% of material would be 'over-blocked.' The 2009 report by Enex Testlab found 100% accuracy with the ACMA blacklist only, but 3.4% of material was over-blocked when additional content was filtered. With other filtering methods, this figure could reach 20%, meaning one in five web pages may be incorrectly blocked.

While Enex Testlab reports that over-blocking is likely to be minimal for the ACMA blacklist, excessive blocking of other material would adversely affect businesses that are not breaking any censorship laws because of a direct loss of

Chris Williams-Wynn is a recent honours graduate of the University of Melbourne.

Endnotes for this essay can be found at www.policymagazine.com.

customers and a reduced web presence. The stigma associated with censored material may unfairly lead to a further decline in patronage of affected businesses. Consumers paying for internet access also suffer a loss of value because the service they receive is reduced or crippled by legislative action. Though the government has released a discussion paper on accountability and transparency for the creation of an RC blacklist, no formal process of review of further content filtering has been announced.

ISPs will be expected to cover most filtering costs, which they would pass on to their customers.

ISPs will be expected to cover most filtering costs, which they would pass on to their customers through higher prices (or less bandwidth). According to 2005 estimates, the most reliable ISP level filtering would cost at least $79 million to establish, and in excess of $30 million per year to run.[4] Given the larger numbers of both ISPs and internet users now, total costs to the economy would be higher. Further, Enex Testlab's report notes that initial costs, including purchasing and installing the required hardware and software, will vary with the size of the ISP. Thus, this policy puts smaller ISPs at a disadvantage, which may lead to a concentration of the market over time if these ISPs are unable to compete. In the long-run, this may translate into further price rises and decreased bandwidth quotas.

Political concerns

While protecting children is necessary, the blanket approach embodied in ISP level filtering raises freedom of expression concerns. Under the current system, the process for blocking material is opaque. To report websites, users must navigate through the ACMA's website to an area where complaints can be lodged. Although complaints are purportedly investigated before any action is taken, some material is still incorrectly blocked. The process raises the concern that any web content the government considers objectionable could be blocked without warning, explanation or community consultation. Recent information demonstrates errors may also remain undetected and unremedied. Following a leak of the ACMA's blacklist, about 150 websites were reportedly removed, suggesting that their content was reviewed in response to increased public pressure and awareness, not because of existing guidelines.[5] The leak and its aftermath highlight the lack of public review in the current blacklist system: all decisions are made behind closed doors with no requirement that reasoning be published. The only notification to a blacklisted party is a takedown notice directed at the website's host, if Australian.

Lawful content is also threatened by such a system. Other banned content included political material, opening the window for dissenting opinion to be blocked. Artists involved in the creation of provocative, though legal, pieces should also be concerned, as anonymous arbiters of taste and decency would be able to restrict their exposure to the broader public.

The government has recognised that more accountability and transparency is necessary, with a December 2009 consultation paper setting out various options. One proposal is that ACMA refers material it believes is RC to the Classification Board, where there is an existing process that allows content producers to appeal against ratings decisions. ACMA could be required to notify content owners of RC ratings, though it is not always possible to identify who is responsible for a website. Another option is to have a standard 'block page' that would appear whenever an internet user tried to access a URL on the blacklist. That would give the user an opportunity to appeal against the classification, or to publicise unnecessary censorship. The options canvassed allow for greater participation in the filtering process and provide a voice for affected parties.

At present, publication of the blacklist is illegal, and there is no proposal in the government's discussion paper to publish it. Under a live filtering system, it is unclear why Universal Resource Locator addresses (URLs) of inaccessible blacklisted sites could not be posted in the public domain and accompanied by reasons for banning these websites. This approach would go further than the consultation paper's suggestions, and encourage public debate over the blacklisting of websites to ensure that censors are accountable.

Policy alternatives

Even if censorship concerns can be overcome, live filtering is likely to impose significant costs on law-abiding internet users without necessarily shielding children from all unsuitable material. An alternative approach, in place until the end of 2008, allowed households to control access to web-based material through their own filtering software, which was provided at no cost by the government. This approach empowered households to decide what constitutes inappropriate material without unduly hampering the connection performance of the approximately two-thirds of households without children under fifteen.[6] The combination of the ACMA's centralised (albeit imperfect) system for tackling illegal content with a decentralised approach to filtering both recognised the multiplicity of opinion among the population and offered parents a low-cost means of protecting their children. The blanket ISP level filtering approach proposed by the government assumes that when judging internet content, one size fits all.

An alternative to strict censorship is more proactive education of the public. A decentralised approach to the viewing of legal internet content could be complemented by a campaign promoting public awareness of internet risks. Relevant information regarding dangers on the internet, such as use of chat rooms, could be disseminated to the public through a variety of channels. Such a policy puts responsibility for what children see on the internet in the hands of parents, while providing them with the knowledge to make informed decisions. This educational approach is favoured by various organisations, including those representing the rights of children, as evidenced by a recent joint statement.[7]

One aspect of the government's planned approach is positive, but could be implemented without also introducing ISP level filtering. Additional funding is to be made available to the Australian Federal Police to investigate child pornography.[8] Providing additional resources to professionals trained in identifying and tracking alleged offenders is likely to succeed where a filter will fail, namely in regard to instant messaging and peer-to-peer protocols. In the case of instant messaging, a crude filtering method involves comparing intercepted content with lists of keywords to be blocked, but this requires large amounts of computer processing power and depends on the lists being kept up-to-date.

The widespread availability of software for encrypting data further reduces the efficacy of filtering because additional information, such as passwords, is needed to analyse the data. An article from an anonymous, self-professed child pornography participant highlights how difficult it is for police to discover and dismantle child pornography rings because of the latter's use of sophisticated security measures.[9] While computer-based filtering operates passively within defined rules, police are able to actively infiltrate and dismantle criminal groups. Indeed, in Enex Testlab's report fewer than 20% of attempts to circumvent the ACMA blacklist were successfully blocked, casting doubt on the usefulness of such a scheme for preventing access by technically savvy individuals. Investigative policing is more likely to succeed than a scattershot, nation-wide filter relying on inflexible computer protocols.

Conclusion

Mandatory internet filtering is likely to be unpopular. A 2007 survey conducted by Whirlpool Broadband Multimedia of informed and frequent internet users in Australia found that only 14.4% of 17,881 respondents indicated that they agree or strongly agree with such a filtering scheme.[10] In 2008, a survey of 19,763 respondents found more than 85% said they would opt-out of a filtering mechanism if possible.[11] Although approximately 70% of survey respondents in the 2009 Enex Testlab report stated they would 'probably or definitely continue to use this service,' some customers already used a filtered service from their ISP. Thus, the sample contained some bias, leaving the level of general support for such a policy ambiguous. As the economic costs and political concerns associated with mandatory filtering become more apparent to the public, opposition to it is likely to grow.

It is not possible to entirely stop misuse of the internet without affecting legitimate users. Instead of live filtering, more economical and ethical methods could be employed to educate and protect internet users. The police, rather than ISPs, are best placed to indentify and stop child pornographers and other online exploiters of children. Hopefully, the government, or failing that, the Senate, will realise that a generic approach such as mandatory filtering will not solve what is in reality a complex problem.