Filtering Overview

THE LABOR PARTY WENT TO THE 2007 ELECTION WITH A COMPREHENSIVE PLAN FOR "CYBER-SAFETY" - THAT IS, MAKING THE INTERNET SAFER FOR CHILDREN.

The centrepiece of this policy, and its most expensive component, is the controversial national ISP Internet filtering scheme. The filter was, in theory, to protect children by shielding them from age-inappropriate online content, and to prevent the spread of child-abuse material online.

The plan has since changed. In its current form, the plan requires that Australian Internet access be subject to a Government-controlled blacklist comprising content that would be "refused classification" under Australia's content classification scheme. This would certainly include illegal child-abuse material, but the category is much broader than that, including, for instance, content that deals with instruction in crime, drug use, and some adult sexual material. This mandatory filter, along with the new censorship powers behind it, was not an election promise. In the meantime, it has proven a distraction from the bigger priority of delivering faster and more affordable broadband for all Australians.

Despite its stated rationale of protecting children, the policy has been very controversial. Those criticising the filter include ISPs concerned about the technical problems and expense, civil-libertarians worried about the free-speech issues of regulating internet content, and analysts concerned at the expense and ill-defined policy goals.

Opponents don't dispute the worth of providing tools to help parents, but take issue with the expense, side-effects and manifest unworkability of this scheme. It is fair to say that the filter is no longer a cyber-safety tool at all, as the scope and size of the blacklist are too limited to bring parents any peace of mind. For instance, X-rated material will, by definition, not be included on the list. The implementation of such a list could only give parents a false sense of security. This calls the entire rationale for the scheme into question.

Furthermore, there are many concerns around the government administration of the scheme. Details remain scarce, but it is hard to imagine a mechanism by which a government agency could administer Internet content regulation in a transparent, efficient and timely manner, especially when the list is a secret one. In any case, as the Government admits, it will be possible for any motivated user to circumvent the filter if desired.

Instead of an expensive and unworkable national cheme, we propose a renewed focus on parental education and supervision combined with continued support by government and industry for PC-level filters that can be tailored to individual families as desired.

The real risks children face online - just as in the real world - stem from interactions with others. With the help of parents, children need education to become safe and responsible citizens online and off.

Main Concerns

- The filter will not protect children from inappropriate material
- The filter will not prevent criminals from accessing and distributing child sexual abuse material
- The filter will block access to material that is currently legal to possess and view, just not to sell and publicly display

Electronic Frontiers AUSTRALIA

PO Box 382, North Adelaide SA 5006
T +61 2 9011 1088 F +61 2 8002 4009
E email@efa.org.au W www.efa.org.au

Cyber-Safety

THE LABOR PARTY WENT TO THE 2007 ELECTION WITH A POLICY DOCUMENT ENTITLED "LABOR'S PLAN FOR CYBER-SAFETY".[1]

In this document, Labor identified a number of risks children faced online and outlined a plan for addressing them. Mandatory ISP-level Internet filtering forms the core of this policy aimed at keeping children safe online.

The same document highlighted some of the risks children face online, including:

- online identity theft;
- cyber-bullying;
- having photos published online without their permission;
- computer addiction;
- picking up a virus or trojan;
- online activities of child predators; and
- inadvertently downloading illegal content when file-sharing.

In fact, ISP-level Internet filtering addresses none of these risks. Filtering is aimed at mitigating so called "content risks" - the risks associated with accidental or deliberate exposure to material inappropriate for minors. It is generally agreed, even in the Government's own research, that these risks are among the least significant children face online: "online risks have shifted from content risks associated with the use of static content to include communication risks associated with interaction with other users."[2]

Labor's plan to tackle inappropriate material is complicated by a choice to attempt to do so at a national and ISP level. What constitutes "inappropriate" is difficult to define, and differs markedly between children of different ages and between different families. Since the Web constitutes billions of web pages and is constantly changing, it is not feasible to classify the Internet as we do movies and books. Therefore, effective filtering software must examine what users are browsing and decide in real time what is appropriate and what is not. Such software, however, is notoriously inaccurate and has an enormous impact on network performance (see "Technical Issues" fact sheet).

A recent report by Harvard University concludes that the risks to children are, in general, overblown. On the subject of inappropriate material, the study's authors conclude that "the Internet increases the availability of harmful, problematic and illegal content, but does not always increase minors' exposure. Unwanted exposure to pornography does occur online, but those most likely to be exposed are those seeking it out, such as older male minors."[3] Because of the ever-changing nature of web content and the ease with which filters are bypassed, an ISP level filter is unlikely to prevent those who are determined to find such material from accessing it.

> "Online risks have shifted from content risks associated with the use of static content to include communication risks associated with interaction with other users."

The authors state that governments should resist endorsing particular technological solutions: "Technology can play a helpful role, but there is no one technological solution or specific combination of technological solutions to the problem of online safety for minors." Instead, "parental oversight, education, social services, law enforcement, and sound policies by social network sites and service providers"[4] are the only ways to achieve an outcome for the safety of children. Tellingly, the task force received no submissions for ISP-level filtering products.

EFA applauds the Government's commitment to cyber-safety. Unfortunately, the national filtering policy is over-reaching in its goal to render the internet safe for children through filtering and classification. Parents still have the option of installing effective and customisable filters in their homes. Existing research, expert opinion and common sense indicate that better outcomes are to be expected from parental education and empowerment than from a government-mandated filter.

1 http://www.alp.org.au/download/now/labors_plan_for_cyber_safety.pdf
2 Developments in Internet Filtering Technologies and Other Measures for Promoting Online Safety, p 1.
3 Berkman Center for Internet and Society at Harvard University, Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force, p. 5.
4 Ibid., p. 4

Electronic Frontiers AUSTRALIA

PO Box 382, North Adelaide SA 5006
T +61 2 9011 1088 F +61 2 8002 4009
E email@efa.org.au W www.efa.org.au

Technical Issues

ISP-based filtering is likely to degrade performance and increase cost, and is unlikely to effectively restrict access to the majority of child abuse content, which is predominantly distributed through illicit encrypted channels.

THE GOALS OF THE FILTERING SCHEME ARE VERY DIFFICULT TO REALISE TECHNICALLY.

The reasons are not hard to imagine. Keeping kids safe requires more than just filtering out adult content, which itself is a very difficult problem given the vast quantity of material on the Internet. On the other hand, preventing the spread of illegal material is a problem that is already being tackled by law enforcement. The traffickers of such material will not be inconvenienced by a filter.

Filtering can only realistically be performed on web content. However, the majority of Internet traffic is now in other protocols - email, chat and peer-to-peer applications. This is particularly true for so-called 'illegal' content.[1] Filtering will not apply to these technologies, and therefore will neither mitigate the risks to children associated with them, nor impinge on their use for illegal purposes.

The Internet is a network, not a broadcast medium. For this reason, Internet traffic can take a variety of paths to reach its eventual destination. This fundamental fact means that almost any conceivable filter can be easily circumvented. If traffic to and from a web site is blocked, any user can have that data sent via a non-blocked third party server using a proxy, VPN or other service. Once any filter is in place, it will be bypassed instantly by anyone who cares to, though any performance penalty will still apply. Regulating broadcasters is simple because there are a limited number of speakers. Regulating a distributed system requires a much more sophisticated approach, and is in many cases not feasible.

Dynamic Filtering

Dynamic filters, tested by the ACMA, are the most aggressive type of filtering, in that they do not rely on a pre-compiled black list but examine content as it is requested and compare it against a list of filtering criteria. While appropriate for an individual PC or workplace, these sorts of filters are not appropriate at a national/ISP level. The performance degradation is severe (on average 30% in the ACMA test under ideal conditions [2]), and for every hundred web pages requested, several will be mistakenly blocked even by the most accurate filter ('false positives'). Dynamic filtering is inherently unreliable as technological measures are inferior to human judgement; for example, educational sexual health resources are often inappropriately blocked by dynamic filters. Furthermore, proscribed content will regularly be let through ('false negatives'), eliminating any cyber-safety benefits. In short, the technological challenges of such filters are so great that even the most repressive censorship regimes rarely use them.

Performance will always be a concern. The main function of an ISP is the routing of Internet traffic, which is a highly optimised process. In general, at no point in the routing process does the hardware or software involved examine the contents of the data packets. To do so requires enormous computational resources (analogous to having the post office read all the mail before delivery). For this reason, it is inevitable that any dynamic filtering scheme will result in a performance degradation or cost increase, probably both.

URL-Based Filtering

URL filtering - blacklisting - blocks access to content on a pre-determined list of web addresses (URL stands for 'Uniform Resource Locators'). To the extent that URL-based filtering is technically feasible, it suffers from some severe inherent limitations. There is an enormous administrative overhead in compiling a large and accurate list of content that is deemed to be prohibited. This suggests that either a very large team of highly trained bureaucrats will be required to oversee the continued accuracy of such a list, or that the creation and maintenance of the list will be outsourced to international organisations that are not accountable to the Australian public. Due to the many billions of web pages in existence, only a miniscule fraction of internet content could ever be reviewed under such a scheme. (The current ACMA blacklist is compiled based on complaints from the public and contains just over 1,000 web addresses.)

There is also a substantial problem with URL based filtering given the constantly changing nature of the web. Sites that host blocked (and 'illegal') material are likely to have a large incentive to change their URLs often in order to avoid the filter and detection by the authorities. The rate at which these sites are able to change their URLs suggests that URL filtering is unlikely to be particularly effective at blocking the most objectionable content on the World Wide Web.

While simpler than dynamic filtering, URL-based filtering has its own technical challenges. Filtering based on the domain name or IP address of the remote server is more efficient, but will block access to all web pages on that site instead of merely the blacklisted pages. Therefore a more subtle and complex process must be undertaken by the ISPs. This can be expensive and have unintended side effects, such as the inability of users in the United Kingdom to edit Wikipedia pages after a single article was added to a blacklist there.[3]

Encryption and Security

Our digital economy relies heavily on encrypted connections to ensure the security of banking, e-commerce and private information. Such connections are secure because the data is encrypted at all stages between the user's PC and the remote web server, and cannot be deciphered even if intercepted by a third party at the ISP.

This model is completely at odds with the filtering proposoal, which requires an inspection of all data going between the user and the remote web server. As a consequence, the filter must either ignore encrypted traffic, making circumvention even easier than before, or break the e-commerce security model by preventing encrypted connections between users and their financial institutions. Neither outcome is desirable.

1 See Fact Sheet: Combating Illegal Material for more information.
2 ACMA: Closed Environment Testing of ISP-Level Internet Content Filters p. 39
3 http://www.guardian.co.uk/technology/2008/dec/08/amazon-internet-censorship-iwf Wikipedia row escalates as internet watchdog considers censoring Amazon

Electronic Frontiers AUSTRALIA

PO Box 382, North Adelaide SA 5006
T +61 2 9011 1088 F +61 2 8002 4009
E email@efa.org.au W www.efa.org.au

Filtering Overseas

It remains true that, should the mandatory filter go ahead, Australia would be joining an undesirable group of countries where the government can, by fiat, restrict any citizen from viewing a particular web site.

THE GOVERNMENT HAS JUSTIFIED ITS COMMITMENT TO INTERNET FILTERING PARTLY WITH COMPARISONS TO SUPPOSEDLY SIMILAR SCHEMES IN OTHER COUNTRIES.

Many of these comparisons have been highly misleading. Mandated, technological filtering regimes are very uncommon in democratic countries. The oft-cited examples of the United Kingdom and Scandinavia are on a very small scale, are opt-in, and run voluntarily by ISPs rather than by legislative requirement. They are therefore not comparable with what is currently planned for Australia. None of these countries has implemented anything analogous to a child-friendly ISP-level filter.

Comparisons have been made to countries such as China and Iran whose Internet access is highly censored. The Government takes umbrage at such comparisons. Since they have no plans to block dissenting political views, they see these comparisons as disingenuous. Filtering opponents have made no suggestion that the filter is targeted at political speech, only that mandatory, government-controlled censorship of the Internet is rare in democratic countries. It remains true that, should the mandatory filter go ahead, Australia would be joining an undesirable group of countries where the government can, by fiat, restrict any citizen from viewing a particular web site. Those countries that do have a technological censorship in regime in place tend to place more importance on silencing dissenting views or safeguarding public morality than ensuring good network performance or digital entrepreneurship.

Very few countries, even those such as Iran that censor the Internet zealously, have implemented dynamic content analysis at an ISP level. Some regimes filter based on keywords in web addresses, but real-time monitoring of requested page content is very rare (China may be the only country do to so, and in a limited way). This indicates how difficult such a scheme is to implement technically (see Fact Sheet: Technical issues.) No other country requires the provision of optional ISP-level filtering for families.

COUNTRY	MANDATORY FILTERING?	FILTERING DETAILS
United Kingdom	No	Government specifically excluded from online censorship by the Communications Act. British Telecom has implemented a private, voluntary clean feed system. A number of ISPs voluntarily use the Internet Watch Foundation's blacklist.
Canada	No	Eight ISPs, without Government coercion, run a voluntary parental control tool. The project states that "There is no legal obligation to do this; it will be entirely voluntary." ISPs may have technical or other reasons for not adopting the system.
Sweden	No	One ISP, Telenor, runs an optional blacklist. It was embroiled in controversy last year when the police tried to add P2P trackers to the list as child pornography sites.
Norway	No	Norway's major Internet service providers have a DNS filter which blocks access to sites authorities claim are known to provide child pornography
New Zealand	No	No Internet censorship exists
Finland	No	ISPs voluntarily apply police-maintained blacklist. DNS only.
Iran	Yes	Huge range of material banned. Internet speeds limited. Commercial filters used, based on keywords and blacklist. No dynamic filtering.
China	Yes	Massive and pervasive Internet censorship, including dynamic filtering.
Saudi Arabia	Yes	Huge range of material banned. Commercial filters used, based on keywords and blacklist. No dynamic filtering.
India	Yes	Certain extremist political web sites officially banned, but enforcement is patchy. Studies show little actual filtering.

Electronic Frontiers AUSTRALIA

PO Box 382, North Adelaide SA 5006
T +61 2 9011 1088 F +61 2 8002 4009
E email@efa.org.au W www.efa.org.au

Combating Illegal Material

Every dollar spent on unreliable technology would almost certainly be more effectively spent funding the operations of proven specialist police forces.

ONE GOAL OF THE MANDATORY TIER OF THE FILTERING INITIATIVE IS TO PREVENT THE SPREAD AND CONSUMPTION OF ILLEGAL CHILD-ABUSE MATERIAL

Preventing the spread of such material is a laudable goal and one shared by EFA. Unfortunately, the fight against child-abuse traffickers will not be aided by the planned filtering scheme.

There is a significant problem with the continued use of the term 'illegal' in reference to Internet content. The Labor government has used the term 'illegal' to refer to child sexual abuse material, for example, but it is clear that the ACMA blacklist contains a large proportion of material that is not child sexual abuse material and is not currently illegal to possess in Australia. In order to clarify the debate, we will use the term 'child sexual abuse material' rather than 'illegal material'.

The extent to which child sexual abuse material is trafficked openly online is often exaggerated, or conflated with material that is only illegal in some contexts, such as X-rated material. It is sometimes claimed that up to 100,000 websites exist offering such material, or that it is a $3 billion a year industry. In reality, the trade is deep underground, and the number of sites is much smaller (from hundreds to a few thousand).[1] The mandatory internet filter is to be based on a blacklist of prohibited websites. However, the vast majority of illegal material that is traded is done so not on the public Internet but among highly secretive networks, who use peer-to-peer and other file-sharing technologies to trade pictures.[2]

Where such material appears on websites, it is actively pursued by law enforcement. Research shows that such websites remain live for a mean time of 30 days.[3] Although this is still too long, and pressure must be applied to the hosts of such material, it seems unlikely that a government-administered blacklist could remain current without significant resources devoted to seeking out illegal content. EFA contends that this task is better left to law enforcement and is not an appropriate task for the media regulator.

The issue is further complicated by as-yet-unresolved questions of who controls the blacklist and how it is distributed. Oversight questions aside (see Fact Sheet: Filtering and Free Speech), the list has already been repeatedly leaked on the Internet, as happened with similar lists from Denmark, Thailand and other countries.[4] This has put the Australian government in the unenviable position of compiling and publicising a list of highly objectionable material.

Technically, it may be feasible to block access to a list of URLs, albeit at some expense to ISPs. However, the way the Internet works guarantees that such blocked sites will be quickly accessible using one of various tools to circumvent the filtering (see Fact Sheet: Technical issues.). Those who habitually seek out illegal material are technically sophisticated[5] and will not be inconvenienced by a blacklist filter. Therefore, the only effect the filter would be likely to have would be to prevent accidental access to illegal material. (Indeed, this is the only stated goal of the U.K's own "clean feed" system.[6]) EFA is aware of no evidence that suggests that Internet users are accidentally stumbling across an epidemic of such highly illegal material. Although preventing such accidental access would be desirable, the financial and other costs (such as mistaken blacklisting and leaks of the list itself) of filtering indicate that better results would be had devoting the resources elsewhere.

A national filter will not slow down the production or consumption of illegal child abuse material. A well funded investigative police force continues to be the best method to combat the trade in such material. The current budget realities suggest that every dollar spent on unreliable technology would almost certainly be more effectively spent funding the operations of specialist police forces. Instead of increasing resources available to the Australian Federal Police, the Government has reportedly slashed $2.8 million from the budget of the AFP's Online Child Sex Exploitation Team in cost-cutting exercises.[7] EFA strongly believes that the Australian Government should be investing in the proven capacity of its trained police force rather than in ineffective and unreliable technological measures.

1 See Irene Graham, Statistics Laundering: false and fantastic figures for a thorough analysis of trafficking statistics.
2) http://www.schneier.com/blog/archives/2009/03/the_techniques.html
3) "The Impact of Incentives on Notice and Take-Down", p. 7.
4) http://www.somebodythinkofthechildren.com/denmark-net-censorship-blacklist/comment-page-1/
5) http://en.wikipedia.org/wiki/Child_pornography
6) http://www.guardian.co.uk/technology/2005/may/26/onlinesupplement
7) See Darren Paulli, "Federal police anti-porn operations cut by razor gang", Techworld (10 June 2008) <https://www.techworld.com.au/article/224056/federal_police_anti-porn_operations_cut_by_razor_gang>.

Electronic Frontiers AUSTRALIA

PO Box 382, North Adelaide SA 5006
T +61 2 9011 1088 F +61 2 8002 4009
E email@efa.org.au W www.efa.org.au

Filtering and Free Speech

CIVIL LIBERTIES ADVOCATES INCLUDING EFA REGARD THE GOVERNMENT'S FILTERING PROPOSAL WITH DEEP SUSPICION, WARY THAT THE DRAWBACKS OF NTRODUCING A NEW CENSORSHIP POWER GREATLY OUTWEIGH ANY BENEFITS

Many questions remain about how content will be Regulated under the proposed two-tier filtering regime, but enough is clear to reveal some serious problems.

Ineffectiveness

The World Wide Web contains billions of web sites and millions change on a daily basis. Any scheme that relies on blacklisting or categorisation of web sites faces an impossible task in keeping up. Any list is likely to be rendered more inaccurate because the material most likely to be censored is also the most likely to appear, disappear, and change locations on a rapid basis. The blacklist of "prohibited content" compiled by the media regulator, ACMA, which would form the initial mandatory blacklist, is produced in response to complaints and hence is so small as to have no useful effect. It is not clear how any complaints-driven or human-vetted blacklist can possibly scale to levels where it would make any noticeable contribution to preventing accidental access to unwanted material. The alternative, dynamic filtering, is slow, expensive and too inaccurate to be practical at a national level.

The Scheme Covers Material Legal in Other Media

Claims that the scheme will only cover "illegal" material are manifestly false. Despite the limits of the ACMA blacklist, it appears that only around half of the items on it consist of material that it is illegal to possess.[1] Additionally, the ACMA list potentially includes a vast range of material: material that ACMA considers likely to be Refused Classification by the Classification Board; material that would be rated X-18+; material that would be rated R-18+ and is not protected by a Government-approved age-verification mechanism; or even, under some circumstances, material that would be rated MA-15+ . If we consider its potential scope rather than its current composition, the overwhelming majority of the content that could be blacklisted by ACMA is material that in other media can be legally purchased (and remains legal to possess) in Australia. A recent leak of the current ACMA blacklist confirmed many fears when it revealed that gambling sites, euthanasia information, and a page dedicated to photographer Bill Henson were among hundreds of perfectly legal but controversial sites listed.

Secrecy and Lack of Accountability

Internet censorship is difficult to achieve in a manner consistent with an open democracy. The ACMA blacklist is secret, unaccountable, and unappealable, whereas other forms of content are examined by a Classification Board whose decisions are open to scrutiny and appeal. The ACMA list is not published and has even been specifically exempted from Freedom of Information requests. While publishers in Australia may receive a takedown notice following a complaint to ACMA, publishers overseas will receive no notification and may not even be aware that Australians are being blocked from accessing their content. It is not known what information will be provided to Australians who attempt to accessed blacklisted material - so when material is incorrectly or inappropriately blacklisted, no one may know.

Furthermore, as the list has been repeatedly leaked, it severely undermines the stated goal of preventing access to illegal material. The Government has also indicated that it plans to incorporate blacklists from the Internet Watch Foundation.[2] This puts often controversial censorship decisions in the hands of a third party unaccountable to the Australian Parliament, let alone the Australian public. For instance, the IWF made headlines in 2008 after adding a Wikipedia page to its blacklist.[3] While the ban was eventually overturned following public pressure,[4] its implementation by some ISPs interacted with Wikipedia's security policy in such a way that many UK users were blocked from editing Wikipedia.

Australians ought to be very wary of the outsourcing of crucial government censorship functions to international organisations that are not accountable to the Australian public. The risk of wrongful blocking and the lack of transparency and due process are highly likely to outweigh any perceived benefits of the proposed scheme.

Scope Creep

There are concerns that the Government will expand the scope of the blacklist in future. There have already been suggestions by politicians that it be extended to cover hate speech and eating disorders.[5] The Minister himself has acknowledged this as an issue.[6] Filtering also represents a major expansion of censorship from media companies who publish or broadcast in Australia to all creators of Internet content anywhere in the world, which includes ordinary Australian users.

Once a mechanism exists whereby content can be blocked by Government fiat, it will be tempting to expand the list beyond its original scope. Many, including EFA, believe that it is inevitable that political pressure will be brought to bear to expand such a blacklist; indeed, it is already happening. The Australian people expect a strong argument to be made before putting such a tool in the hands of this and future Governments. While understandable, an impractical desire to render the Internet child-safe and to blockade illegal material does not provide sufficient justification.

1 Commonwealth, Parliamentary Debates (Senate), 03 February 2009, Question No 833, p 192 <http://www.aph.gov.au/hansard/senate/dailys/ds030209.pdf>.
2 http://www.dbcde.gov.au/communications_for_consumers/funding_programs__and__support/cyber-safety_plan/internet_service_provider_isp_filtering/isp_filtering_-_frequently_asked_questions
3 http://www.guardian.co.uk/technology/2008/dec/08/amazon-internet-censorship-iwf
4 http://www.guardian.co.uk/technology/2008/dec/09/wikipedia-iwf-ban-lifte
5) http://newmatilda.com/2008/11/11/should-pro-ana-sites-be-banned
6) http://www.cio.com.au/article/296842/url_blacklist_creep_possible_conroy?eid=-60

Electronic Frontiers AUSTRALIA

PO Box 382, North Adelaide SA 5006
T +61 2 9011 1088 F +61 2 8002 4009
E email@efa.org.au W www.efa.org.au