

November 2, 2008

Hon Kevin Rudd MP
Prime Minister
Parliament House
Canberra ACT 2600

Dear Prime Minister,

RE: Mandatory Australian Internet Censorship / “Clean Feed”

I write this letter as one of your constituents in the Griffith electorate, and hope to express my genuine concern for the Australian Labor Party’s plans to introduce mandatory Australian Internet Censorship in Australia. I believe this policy represents a great step backward in Australian policy and telecommunications law. I urge you to reconsider your position on this important issue.

I will preface this letter by stating that:

1. I have been using the internet nearly every day since 1994;
2. I have been following the recent discussions on internet censorship very closely;
3. The debate of mandatory internet censorship has been polarised by many participants who suggest that those opposed to the changes support child pornography; and
4. I have no interest in accessing any child pornography or other illegal content.

While I understand that it is difficult to satisfy everyone with such a contentious issue, the Australian Labor Party has not demonstrated a need for mandatory filtering. The Australian Labor Party also failed to advise that it would implement mandatory filtering for all citizens prior to the election. Such a major shift to the status quo should be implemented after the people have had the opportunity of electing a party based on the proposal.

In any event, where a change is proposed to a position successfully adopted for years, the government should give due consideration as to whether there is a real advantage resulting from the changes and if the balance of convenience favours the change. As I will demonstrate, the “clean feed” proposal satisfies neither.

The previous Australian Government has already taken steps to ensure that internet filtering software is available freely for citizens to use (through the NetAlert program). While this program is not heavily utilised – perhaps because the need for censorship software is not deemed to be essential, this is a step in the right direction. Children can (and should) be protected by some of the evils online; however, mandatory filtering imposes unreasonable restraints upon the public.

While I understand the issues facing concerned parents today, and the impact of unfiltered internet access upon their children, the most efficient and accurate method of ensuring internet usage is appropriate for children is for close parental supervision. Software (whether installed on the child's computer or at the internet service provider tier) is unable to accurately detect all unsuitable content (nor guarantee legitimate traffic is not blocked) and is no close substitute for appropriate parenting.

My objections to the policy imposing mandatory filtering are detailed below, but can be summarised as:

1. The Government misrepresented that the filter would be opt-out prior to the election;
2. The ideals of a representative democratic society oppose censorship;
3. Decisions to place a site on the blacklist are not accountable to the Australian public;
4. Making a "blacklist" may make illegal content easier to access and enable the abuse of children;
5. Filtering introduces delay and declined performance in internet traffic;
6. The filters are inaccurate and often incorrectly block legitimate traffic;
7. Introducing filtering creates another device in our Internet hierarchy that is subject to failure, introducing a greater chance of failure and Internet outages;
8. Filters cannot filter all protocols, or even the majority of internet traffic;
9. Filters may cause those viewing child pornography to take further steps to ensure their traffic is better protected (encryption, anonymisers such as TOR), further hindering law enforcement officers;
10. Filters may lull parents into a false sense of security regarding online content;
11. Filtering HTTPS (SSL) connections may introduce a level of insecurity in "secure" Internet connections;
12. The costs spent in implementing the filters can be better spent elsewhere;
13. Children aware of the filter will deliberately attempt to find filtered sites and bypass the filter;
14. Australia's top Internet Service Providers oppose the proposal; and
15. There are more appropriate methods to prevent societal problems and to protect sensitive individuals from offensive or illegal material.

The Government misrepresented that the filter would be opt-out prior to the election

Prior to the federal election, representatives from the government were widely reported as stating that any censorship regime would be based on an "opt-out" system.

The earliest I can find a source of reporting that the censorship regime would be compulsory was in December 2007, well after the federal election in November 2007.¹

I am not representative of the entire population, however, I certainly feel misled. No political party should ever underestimate the effect of implementing such a wide-reaching, heavy-handed proposal after misleading voters prior to the election.

The Ideals of a Representative Democratic Society Oppose Censorship

“When governments start covering the eyes and ears of the whole nation, however, there is a real problem. We only need to look at those governments that have taken it to the extreme and burnt books to understand that. But there are more subtle ways to inhibit the flow of ideas that we need to be just as alert to.” – Kate Lundy, Australian Labor Party Senator.²

Democracy is based upon the fundamental principle that the citizens have an ability to be aware of the issues facing their society, and have the freedom to vote for a representative government from these informed views. In fact, it is difficult to reconcile the “freedom of political communication” found by the High Court of Australia in *Australian Capital Television v Commonwealth of Australia (No 2)*³ to a law that could allow the government to arbitrarily blacklist any website from all Australians. Further, in recent times, governments have made legislative changes to promote transparency and accountability to its constituents (I refer to both Commonwealth and State Freedom of Information legislation, judicial review, and other advancements to recognise other aspects of natural justice).

If the Australian government introduces mandatory internet filtering, the average Australian’s ability to access information will be obstructed. In an information age, this should not be taken lightly. Even if this policy is introduced with the best intentions no-one can guarantee that legitimate sites won’t be blocked, nor will the list of blocked sites be available for review by average Australians. This will further empower the government through a disparity in information by withholding information from its citizens.

While comparisons between the proposed Australian filter and China are perhaps a little far-fetched, the amount of political sites blocked from within China should concern any member of society that seeks to stay informed about issues worldwide.

Even in the event that censorship is implemented, the government should not allow free, responsible adults to determine what we can and cannot view in the privacy of our homes.

¹ “Conroy announces mandatory internet filters to protect children”, 31 December 2007, <http://www.abc.net.au/news/stories/2007/12/31/2129471.htm>.

² “Classification, not Censorship”, Kate Lundy, <http://www.smh.com.au/articles/2003/07/29/1059244609141.html>.

³ (1992) 177 CLR 106.

Decisions to place a site on the blacklist are not accountable to the Australian public

While it is uncertain whether the material that is mandatorily blocked will include pornography or online gambling sites, I will assume a more conservative position – that only “illegal” material is blocked. This idea is inherently flawed as no computer system can accurately determine illegal content, and the blocking can only occur by way of a “blacklist”.

Such a blacklist would presumably be maintained by the government, and as yet, it is unclear as to how the government could guarantee the blacklist would not be subjected to political stunts or other bad faith blockings. It is not inconceivable that the government in power may attempt to suppress material critical of that particular government, similar to what has occurred in Norway to Matti Nikki, a blogger critical of Finland’s internet filtering.⁴

Making a “blacklist” may make illegal content easier to access and enable the abuse of children

By creating a blacklist of illegal material that should not be accessible in Australia, the Australian government is creating a central list of websites with such material.

I repeat – *the government will be distributing a list of websites with illegal material, including child pornography.*

If this list were to be released by an unscrupulous individual (which is not unforeseeable, given it will likely be distributed to every Australian Internet Service Provider), it would be the Australian government’s fault, and rightfully so, as there was no demonstrated need to create such a list in the first place.

The “clean feed” internet censorship proposal enables child abuse.

Filtering introduces delay and declined performance in internet traffic

The ACMA report considered performance in limited detail when evaluating modern filtering software and hardware. However, I find the following points extremely concerning:

1. The report took the best aspects of each product tested (accuracy and speed) and failed to adequately report that it is impossible to have one filter that had both the highest accuracy and the highest speed reported (as they are two different products);
2. The test did not appear to replicate real-life conditions that would be experienced by real-life Internet Service Providers – in fact, any given filter would have far, far more clients behind it than was emulated in the ACMA testing; and
3. In any event, if the filters can scale for further users, the cost of additional filters (to handle even more users) will ultimately be borne by the taxpayer.

I am no expert in this particular field, but if these points are obvious to me, then it is evident that the research performed by the ACMA is flawed.

⁴ “Lapsiporno.info and the Finnish Internet censorship”, <http://www.lapsiporno.info/>.

The filters are inaccurate and often incorrectly block legitimate traffic

Filtering of internet access methods is not a new phenomenon, as it has been used by corporations and schools for years. However, these filters can be distinguished easily from nationwide filtering as there is no such thing as “one size fits fall” filtering.

The fact that the ACMA report demonstrates that it is impossible to have 100% accuracy alone should be enough to not proceed with this proposal.

In today’s information age, reliable, fast internet access is essential. This can be confirmed by the Australian Labor Party’s election promises toward a National Broadband Network. Settling on an inaccurate filter system (or in fact, any at all) puts Australia at a disadvantage to other countries that do not have the same limitation.

Introducing filtering creates another device in our Internet hierarchy that is subject to failure, introducing a greater chance of failure and Internet outages

Introducing another device that internet traffic must pass through will reduce the reliability of Australia’s internet access.

Has the government suitably considered what should occur if a filter fails due to hardware failure? Should Australians tolerate an internet outage, when simple client-side filtering software (or for networked computers, a local network filter) would have performed the job properly?

Filters cannot filter all protocols, or even the majority of internet traffic

A study performed by ipoque in 2007 revealed that approximately 73% of all online traffic is peer-to-peer traffic.⁵

Given this statistic, it is interesting that the study of effectiveness of internet filters was confined to HTTP and HTTPS traffic, which account for substantially less than the majority of internet traffic. If the aim of this policy is to protect children, then clearly client-side software capable of filtering encrypted communications at the end-point is far more effective than a “one-size-fits-all” filtering solution imposed upon the public at large.

Filters may cause those viewing child pornography to take further steps to ensure their traffic is better protected (encryption, anonymisers such as TOR), further hindering law enforcement officers

If mandatory filtering of illegal content is introduced, then those wishing to access this content will find alternative means to access the material.

These alternative means include widely publicised methods such as encryption and anonymiser networks (such as TOR) to get anonymous access to a country that does not impose the same laws

⁵ “Internet Study 2007”, Ipoque, <http://www.ipoque.com/resources/internet-studies/internet-study-2007>.

as Australia, and re-route their traffic through such a node. These products will hinder law enforcement by making it far more difficult to catch an offender.

This filter will hinder law enforcement by ensuring that offenders use more robust methods to access illegal material.

Filtering HTTPS (SSL) connections may introduce a level of insecurity in “secure” Internet connections

The recent ACMA study investigating internet censorship solutions suggested that HTTPS traffic can be filtered. HTTPS traffic differs from ordinary HTTP traffic by utilising encryption at the remote server to ensure that the client is communicating directly with the server, and that no other server is “listening in” to the communications (ie, a man-in-the-middle).

It is unclear from the ACMA report exactly how the government plans to censor HTTPS traffic. Either the filtering is done by a blacklist ban of destination IP addresses, which may block legitimate material, or it is filtered by content analysis.

If HTTPS connections are censored by content analysis, the filter between the user and the remote server must have the ability to decrypt the encrypted communications. Communications over HTTPS are typically reserved for secure communications such as credit card details and sensitive personal information.

If HTTPS connections are censored by destination IP addresses, how does the Government determine that servers on the said IP addresses are not also hosting legal content?

It is extremely concerning that such a fundamental to the growing industry of e-Commerce may be compromised by the Australian government and such little consideration seems to be given to this point.

Filters may lull parents into a false sense of security

The only perfect method of ensuring children do not access inappropriate material online is for careful supervision. Even if the government implements compulsory filtering, it cannot guarantee that the material available will be suitable for children (even with the opt-out filters).

Not all parents will understand this, and will rely upon the government filters to filter inappropriate material for them, as a substitute for adequate supervision. This is the exact opposite effect of what the government seeks from the filtering proposal in the first place.

The costs of implementing filtering can be better spent elsewhere

Implementation of a nationwide internet filtering system will cost taxpayers in excess of 40 million dollars. Given there is already free filtering software available, and there is no demonstrated need for compulsory internet filtering (or even national network-wide opt-out filters), this money is effectively wasted by duplicating functionality already provided by the NetAlert program.

Children aware of the filter will deliberately attempt to find filtered sites and bypass the filter

Children may become aware of the filter and will deliberately attempt to discover what sites are banned and are not banned if it is implemented. This is effectively more dangerous, as it has drawn the child to attempt to look for illegal material to discover how the filter works.

This possibility is not far-fetched given the likelihood that parents will become more complacent of child supervision on the Internet if such a filter is implemented.

Australia's top Internet Service Providers oppose the proposal

The government appears to fail to give any consideration to views put forward criticising this proposal. It is extremely concerning that those who would be forced to comply (Internet Service Providers, such as Bigpond, Internode, and iiNet) with such a proposal have come out openly to criticise how the proposal "*won't work*".⁶ What is most concerning about this is that these organisations have spoken against the proposal, and they have a superior understanding of technical know-how to government, particularly a government that appears to be unable to make any headway on a National Broadband Network.

There are more appropriate methods to prevent societal problems and to protect sensitive individuals from offensive or illegal material

Societal problems begin by poor parenting, and there is little evidence adduced by the Federal Government suggesting that societal problems have increased since the internet has become common.

The most appropriate action would ensure parents take responsibility for their own children (rather than continually expecting the government to introduce poor policies justified by "*think of the children*"), introducing tougher penalties for young offenders, and an increase in penalties towards parents of such children.

Conclusion

Given the reasons explained above, the Federal Government would be reckless to implement the proposed "clean feed" mandatory filter. I strongly suggest the Federal Government reconsider its position on this issue as there are many voters with extremely strong views on this issue. I will remember this issue when I return to the polls for the next federal election, as will many others.

In today's world, information is critical. Creating legislation willy-nilly that hinders Australia's access to information will put Australia at a significant handicap in the years ahead.

I will continue to monitor this issue with great concern and would greatly appreciate a considered response to this letter.

⁶ "*ISP-level content filtering won't work: Insight*", 30 October 2008, <http://www.zdnet.com.au/insight/communications/soa/ISP-level-content-filtering-won-t-work/0,139023754,339292158,00.htm>.

Thank you for the opportunity to be heard.

Yours faithfully,

Rhett Kipps

The above work is licensed under the Creative Commons Attribution 2.5 Australia License available at <http://creativecommons.org/licenses/by/2.5/au/>

Please feel free to link to this work and use the points raised in my post for your own letters.