Bjorn Landfeldt
Associate Professor, School of IT

Parliament of Australia
Joint select Committee on Cyber-Safety

Introduction

This submission is provided as supplementary material for the consideration of the committee in response to an invitation for me to attend a hearing on March 24, 2011.

I am writing this submission in the capacity of Associate Professor at the University of Sydney in the areas of Computer Networks and Telecommunication Systems, limiting my comments to terms of reference points:

i) "the online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles) and stakeholders controlling or able to influence that engagement (governments, parents, teachers, traders, internet service providers, content service providers);" and

iii) "Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) their effectiveness and costs to stakeholders, including business;"

At the hearing, I am of course prepared to give wider opinion in the capacity of a private citizen.

School of Information Technologies
Faculty of Engineering and IT
Room 418, School of IT building
The University of Sydney
NSW 2006 Australia

T +61 2 9351 8962
F +61 2 9351 3838
E bjorn.landfeldt@sydney.edu.au

ABN 15 211 513 464
CRICOS 00026A

THE UNIVERSITY OF SYDNEY

The on-line environment

Over the past few years, as the debate on cyber-safety has taken place, there has been a strong focus on the technical aspects of the Internet and the feasibility to perform filtering of content at the ISP level versus filtering at the end user equipment (often referred to as PC-based filtering). Many voices have been heard and the majority of central aspects have been brought to light. It is not my intention to reiterate the main arguments here, rather, I will try to make the argument that the Internet as communication platform is inherently different to previous systems in some key aspects, which has great impact on the outcome of the present inquiry and which should be considered. Especially, I find that many of the most central arguments need to be put in their correct context before being evaluated, or the conclusions drawn are under threat of being too much influenced by rhetoric and opinion making. An example of this is the unwarranted room the notion of "Internet speed penalties" has been given in media. This is a prime example of how the necessary questions to ask have been left out and a simplistic view of "Speed" has become a central question.

I will return to this issue below, after a brief discussion of the on-line environment Australians, as well as others, currently operate within and are likely to experience in the future.

What is the Internet?

The Internet is not, as is popularly believed, what is accessed through a web browser. The Internet is (put simply) a large number of computing devices connected via communication links all using some common standards such as the Internet Protocol (IP). The Internet itself is not browsable, nor does it contain any information of use to most people or organisations. Instead, the Internet is a platform on top of which a wide range of different services and accessible content can be put. The currently most commonly accessed content reside within one of these services, the world wide web (WWW). However, it is far from certain that the WWW will remain the dominant platform for information exchange and retrieval in the future. It is imperative to appreciate this distinction between the Internet and preceding communication platforms such as Broadcast media and even telecommunication networks, which were all purpose built rather than being generic. The technology underpinning the Internet was devised to allow easy evolution of services, enabling swift changes in usage and rapid innovation.

The current on-line environment

As mentioned above, currently, most people associate the Internet with the WWW. In the current situation, information is largely accessed through web pages that contain text, images and sometimes links to other media or other web pages. However, the landscape is fast changing with newer alternatives fast gaining

ground. In the Australian context, the fraction of peer to peer (P2P) traffic is ever increasing and the uptake of alternative media consumption such as live streaming video and audio is growing.

Furthermore, it is currently most common to access information through personal computers in homes and schools, in work places etc. However, the use of mobile personal devices such as smart phones is rapidly growing, leading to a situation where information can be accessed what researchers in the field commonly refer to as “at anytime at anywhere”.

Put together, the current most common environment in which the Internet is being utilised can be described as being of a static nature, where content largely remains unchanged or incrementally changed, accessed through devices that are static and easy to administrate / manage / supervise. Furthermore, there is every indication that this situation will change in the future, leading to a set of completely new challenges for this committee to consider. It is of utmost importance for the Joint Select Committee on Cyber-Safety to consider how the services on top of the Internet will change over time, what technical challenges and societal changes this will bring and how this may effect the policies the Australian Government put in place to combat the envisaged risks as outlined in the terms of reference.

The future on-line environment

The on-line environment is changing at an unprecedented pace. Only a few years ago there was no Facebook or Twitter, online musical stores or voice over IP connections in our homes. It is impossible to forecast which new services will become ubiquitous in the future but for the immediate future there are some trends that are obvious when glancing at the world around us.

It is important to consider the technological changes to the underlying network fabric and to consider how these may change the nature of services to come. First, the emergence of 3G networks (and especially recent additions such as Long Term Evolution, LTE) coupled with the emergence of true mobile computing devices such as the iPhone, Android phones, the iPad etc. clearly point to a near future where mobile consumption of media will be prevalent. It is widely accepted that such a computing environment is suited to more entertainment, on-demand produced or “ephemeral” data than the current static paradigm brings. In addition, the mobile environment also makes use of location based information and it is very likely that proximity based services will become commonplace in the near future. Second, regardless if the NBN will be rolled out to all Australians, fixed access technologies are fast changing and Australians will get access to higher capacity services in the future. Looking at other countries which already have much more developed infrastructure it is clear that new services and usage patterns will follow. For example, in Scandinavian countries it is becoming commonplace to use streaming TV over broadband connections instead of using

terrestrial broadcast networks, services such as Spotify that allows users to freely stream any music (removing the need to ever again purchase a CD or store music at home) etc. It is clear that the trend is towards richer multimedia experience, moving away from primary text based media. Third, there is a strong trend towards user generated content which is rarely produced for commercial purposes. This content has very low archival value and hence is also highly ephemeral in nature. Most social networking forums, sites such as Youtube and Flickr all fall under this category. Since the information itself has a very short "best before date" it is difficult to index and catalogue such information and just as the majority of Australians would not record, document and index their days (meetings, conversations, activities etc.) such information will merely become ambient consumption of information without archival purpose. Finally and most importantly, currently, user information is mainly stored on local hard drives and optical media (CDs, DVDs) and the network connection is used to access information generated by others and to share information with the rest of the world. However, there are signs of clouds in the sky, this is about to change. For most people it does not make sense to store data locally at home or at school where it is locked down to a physical location and vulnerable to hardware failure, damage through fires etc. Our personal data move out of our homes and into the cloud, and we will become reliant on safe and secure communications to produce, store, access and manage our personal belongings over the public network. This will also mean that in general, people will have to be educated in how to protect themselves and their data from unwanted scrutiny and theft. This also has serious implications for any kind of filtering scheme where users will become good at obfuscating their data and where any kind of filter in effect is peeping into Australians' private data at various level of intrusion.

In conclusion, the future on-line environment bears little resemblance with the current situation; we do not know which new services will emerge and become popular, but we do know the shifts will be swift and strong. Any consideration the committee does should bear this in mind so that formed policies are not obsolete before they take effect.

It is important to appreciate the above details about the on-line environment in order to understand the effectiveness and impact of content filtering as is being proposed currently. Below I will briefly detail the various filtering options and point to some major difficulties in *effectively* implementing filtering without severely restricting the use of on-line information.

Content filter types

In the below discussion, we will divide current filtering techniques into two major categories, list based filters and dynamic content filters. List based filters are the least complex and also provide the lowest effectiveness. Dynamic filters are better

at capturing unwanted information but they are also more complex, leading to significant performance problems.

Note, there exist no current technology that can effectively detect and automatically classify multimedia content (voice, video, images) at any reasonable accuracy at a reasonable complexity cost. What this means is that it is currently impossible to filter complex media and obtain accurate results and it is too costly to even try to do so on a larger scale.

List based filters have been described as being 100 % accurate in various press releases and statements in media and this is true. However, these filters only do what they are told, exactly, and nothing else so the problem with these filters is not that they fail what they are meant to do, the problem is how to tell them what to do. A simplified list based filter operates as follows: look at the address of a requested web page, if address is found in a block list, block access, if not, do nothing. Using list based filters means that there is a necessity for very high levels of manual labour in detecting possible sites to block, investigating if a site should be blocked, distributing information about the addition to the list of blocked addresses, continuously monitoring if there are changes to the content of a blocked site, determining if changes to content means the blocking should be removed or still be in effect, updating filters about the removal of blocked sites etc. This high level of manual work required means that the list of material to block will by necessity become very limited or the resources needed to maintain the list in a reasonable way becomes prohibitive. To make matters worse, there is a necessary time lag in the manual process and distribution of lists to filtering sites. This time lag means that only archival data can ever be targeted by list based filters, and more dynamic or ephemeral data will largely be unaffected by such filters.

It is also noteworthy that it is extremely easy to circumvent list based filters in different ways. It is currently common practice to dynamically generate addresses for data as it may move around or the structure of the data catalogue on which the information resides may change so the exact address to the data can easily change. This leads to a situation where the blocking list needs to be frequently updated to reflect these changes. It is also easy to bypass the filter altogether using various proxy techniques or by encrypting the communication so that the filter is unable to determine which address is being accessed. I do not have any hard numbers how commonly this is practiced among Australians currently, but international precedences do exist. For example in PR China there is a thriving market of selling unrestricted access to residents inside Chinese borders, circumventing Chinese restrictions.

Dynamic content filters aim to determining the nature of content as it passes through the filter in an on-line fashion. These filters have the advantage of not

requiring manual intervention. However, they are also notoriously inaccurate and computationally complex. Given a set of training data it is possible to fine tune these filters to accurately capture certain content. However, as soon as the training set differs from the filtered content, the accuracy goes down leading to missed content (under blocking) or blocking too much (over blocking). These filters are also unable to accurately understanding semantics and meaning of data. For example, such filters cannot understand meaning of written text well. It is very difficult to determine if text deals with the matter of sexual education or pornography based on the semantics of the text itself. It is even harder to analyse the content of richer multimedia and determine what a photo contains, if a video is pornographic or not, if a person is making scones or explosives. Currently, it is easy to obfuscate content so that dynamic filters are rendered useless in being able to correctly classifying the nature of the media. Any attempt in doing so on-line would also incur prohibitive costs and severe performance penalties in terms of end user experience.

Returning to the argument that filters can be implemented that are 100% accurate and there are no performance penalties reported. In the context of what has been outlined in this submission, the statement is semantically true, but the argument is flawed. List based filters only address backwards looking problems, they are very human resource intensive and easily circumvented. It is highly questionable if the very limited benefits they bring warrant the costs involved, especially looking forward to an evolving on-line environment.

Another example where rhetoric has been given too much room is the argument that Internet speeds are unaffected with the implementation of content filters. Again, the statement is semantically true but worthless in the context of the purpose of filtering, expected outcomes and environment in which the filter will operate. In order to determine if a filter is suitable one has to determine if it does a good job, i.e. has significant impact and benefit, and evaluate if the performance compares favourably to any performance penalties imposed. In this context, any test of “Internet speeds” can be conducted in a way that is certain to yield and desired outcome and unless there is a proper disclosure of the properties investigated and what acceptable benchmarks are, the tests are not rigorous and the experimental methodology is not scientific. So far, no tests have been reported on that reflect the reality of the on-line environment in Australia even in the next 3-5 years let alone in accordance with the on-line environment for the next generation Internet users that will have the NBN fully implemented.

I think it is appropriate at this stage to point out at that I was approached last year by the management of CORE, the organisation representing all academics conducting research and teaching in computer science in Australia and New Zealand to issue a collective statement on the matter of filtering. The following

text was underwritten by myself and Professor Lueg from University of Tasmania on behalf of CORE:

> *"The Federal Government has announced its intention to introduce new legislation to compel Australian Internet Service Providers to filter all information transfer in Australia, with the intent of stopping the general public from accessing selected information.*
>
> *CORE, the Australasian association of Computer Science schools and departments, has strong concerns about this policy. It is CORE's view that the proposed list-based filtering will not be effective and brings several risks. It is unlikely to exclude much of the unwanted content; it is inapplicable to many of the current methods of online content distribution; and it has the potential to restrict Internet bandwidth. For these reasons, we believe that a better approach is to form an expert body to help design and implement an approach or scheme that is appropriate for Australia.*
>
> *The Government has decided against mandating dynamic content filtering at the ISP level, a move that CORE supports. Such filtering is only scalable if it is distributed on users' end-systems, and any attempt to centralise it would inevitably lead to performance penalties for both responsiveness and bandwidth.*
>
> *A key concern is the limitations of list-based filtering schemes, which build on reporting by the general public and actioning by a Government-nominated organisation. With the pace and volume at which content is added to the Internet, such lists can only capture a small fraction of the material that would be classified as harmful. Also, the emergence of short-lived data such as live data streams and dynamic content generation, and the use of dynamic addressing, leads to a situation where any given list rapidly becomes inaccurate or obsolete. It is therefore unlikely that any significant protection can be offered by such an approach.*
>
> *The filtering has been proposed as a means of making the Internet child-friendly or child-safe, and there is therefore a real risk that, once the filter is put in place, parents and teachers will become less vigilant in supervising children's on-line activities. This is despite the fact that methods for circumventing the filter are widely known. The Government has proposed to also make resources available to educate the general public about cyber safety, a move CORE fully supports. However, we feel that such education must stress the limited benefits of list-based filtering schemes in order to minimize the risk of lowered vigilance.*

The ease at which a list-based filter can be defeated further limits the effectiveness of any such scheme.

CORE is concerned that the Government has not carried out any study to investigate the mandated filtering in the context of future networking environments. The pilot study during 2009 was designed to replicate well-known properties and no significant new information was presented, although the underlying technology is rapidly changing, in particular due to the National Broadband Network, NBN. Not only will the NBN bring higher data rates and shorter response times, it has the potential to overturn our current Internet habits and pave the way for a much richer multimedia experience. It seems certain that the simple web page with relatively unchanging information will decrease significantly in importance. In addition, user-generated live content and peer-to-peer networks will inevitably mean that the filtering scheme has to evolve and be extended to incorporate other, more resource-intensive filtering mechanisms. CORE therefore sees a tangible risk that the mandated filtering will pave the way for costly solutions that have a negative impact on the NBN.

In addition to the many technical concerns held by CORE, there has been wide reaction from other sections of the community to this form of censorship, around concerns with issues such as freedom of speech, the potential for misuse of the powerful tool of blanket filtering, or whether the scheme does indeed achieve the stated aims. CORE asks the Government to drop its plans for legislation of mandated content filtering and create a broad and inclusive working party consisting of experts from the public sector, industry, and academia who can together properly investigate the many issues associated with such a scheme before a decision is made to mandate its implementation.

CORE sees at best limited benefits from the proposed filtering scheme, and high potential risks if the scheme were to be implemented without proper investigation of the possible side effects."

It should be noted that there exist companies in Australia that offer filtering as a service to customers and where it is well understood that over or under blocking can occur. Since customers are able to make an informed decision about the limitations of the system, the advantages the blocking will bring and the potential disadvantages the negative aspects of mandated filtering disappear. Parents may choose to pay for a filtered service during a period when their children are at a vulnerable age, knowing that for example sex education material or information about the holocaust may be blocked with the knowledge that they can resume unfiltered access at any time they so choose.

The need for education

Education plays a central role in the creation of a safer on-line environment for all Australians. One of the greatest threats to individuals is the sheer amount of information that can be harvested about individuals and the potential negative side effects this may have. Many individuals tend to share information about themselves and their lives in public forums in a much more open and accessible manner that they would face to face. For example, there have been reports on people befriending strangers on Facebook and then broadcasting plans to travel, leaving their homes as prime targets for burglary. There is no clear distinction between crime and cyber-crime since on-line and physical actions are interchangeable and can lead to or fuel each other. Clearly though, there is a set of new dangers and considerations people need to be aware of. New educational opportunities do start to emerge. At the University of Sydney there is now a graduate diploma in cyber-security offered from winter 2011. The diploma is an example of efforts in the academic sphere to educate policy makers and managers about the security aspects of cyber-threats. The government should sanction the development of programs on the topics of cyber-safety and cyber-security for inclusion in the primary and high school curriculums as well as developing easily accessible programs for access by the general public. The by far best prevention of risks on-line comes from education and correct behaviour by the end users. This must also be coupled with clear and easy paths to report any activities that are threatening or illegal, especially for young children.

Concluding remark

Currently, the only reasonable strategy for filtering is to implement solutions on end user equipment. To this end, the Net Alert scheme was a step in the right direction. The fact that the uptake was slow cannot be seen as a reflection of the quality of the solution, but instead a failure to educate the general public about the benefits of filtering. Again, education is key to the successful implementation of any protection scheme against on-line dangers.

To this end, the creation of an ombudsman is a most strategic move. However, there is no obvious need for an Internet ombudsman, the ACMA is most likely

equipped to act on most foreseeable issues; Instead, I propose the creation of a children's ombudsman following the model adapted from the one used in Sweden and which would be a most needed and welcome function in Australian society. The terms of reference of this committee acknowledges the special needs and vulnerabilities of children. It is timely to act on this insight and create a strong voice and lobbyist for children with sanctioned strength to propose legislation through the Australian parliament. As an example precedence, the role of the Swedish children's ombudsman is set out below [1].

> *"The Ombudsman's main duty is to promote the rights and interests of children and young people as set forth in the United Nations Convention on the Rights of the Child (CRC).*
>
> *The agency monitors the implementation of the CRC in Sweden. For instance the Ombudsman submits bills for legislative changes to the Swedish Government and promotes the application of the CRC in the work of government agencies, municipalities and county councils. The agency also disseminates information on the Convention.*
>
> *A key duty of the Ombudsman for Children in Sweden is to participate in public debate, promote public interest regarding key issues, and influence the attitudes of decision-makers and the public. However, the Ombudsman does not supervise other authorities and, by law, may not interfere in individual cases.*
>
> *In order to find out their views and opinions the Ombudsman maintains regular contact with children and young people. The Ombudsman visits children in schools and youth clubs, and children can get in touch with the agency by letter, telephone and through this website.*
>
> *Each year the Ombudsman for Children in Sweden submits a report to the Government. This report addresses the situation of children and young people in the country."*

In addition to the overseeing and lobbying functions, the ombudsman should act as central coordinator for concerns and complaints of children, utilising contact persons in schools and other suitable institutions. The following section is taken from [2], the Swedish Ombudsman for Children's Act Section 7:

> *"The Ombudsman for Children shall report to the social services committee without delay if in the course of his work he receives information to the effect that a child is abused at home or it must*

otherwise be assumed that the social services committee needs to intervene to protect a child. If there are special reasons for doing so, a report may be made to the social services committee in other cases also.

The Ombudsman may give the social services committee all the information that may be of importance for investigating a child's need of protection."

This highlights the central role the Children's Ombudsman plays in not only lobbying and representing the interests of children, but also the protection and coordinating role the Ombudsman plays. All children growing up in Sweden are fully aware of the help and support the Ombudsman provides.

Yours truly

Björn Landfeldt

References

[1] http://www.barnombudsmannen.se/Adfinity.aspx?pageid=7043
[2] http://www.barnombudsmannen.se/Adfinity.aspx?pageid=86