Senator the Hon Helen Coonan
Minister for Communications,
Information Technology
and the Arts

Protecting Families Online
Address to the National Press Club

Canberra
Wednesday June 14 2006

Of the many issues within my portfolio that warrant attention, none is more contentious than Internet pornography.

In many ways it is the most concerning and the least understood.

I believe the subject warrants a great deal more informed debate and discussion as it is surely one of the scourges facing young people and families.

Life has become infinitely more sophisticated since the Internet's arrival but it has also become more complicated.

At each technological leap forward we find another push at the regulatory settings. And at every step we find scammers, con artists, thieves, fraudsters and, worse, paedophiles and pornographers, who can quickly adapt to using more treacherous and sophisticated methods of committing their crimes.

While the Internet is generally used as a tool to broaden our horizons and as an almost limitless source of information, there are pitfalls.

The Internet can be a global playground for the unsavoury and the uncivilised.

And while in Australia we have taken significant proactive action on our own soil, in cyberspace there are many places to hide your location, your identity and your true purpose.

To help protect Australian families, the Government has committed to doing everything reasonably possible to ensure that all Australians – particularly children – are safe on the Internet.

We are of the firm belief that a holistic approach to Internet safety is the best way to protect children.

We need to educate parents, teachers and kids about the dangers of the net, we need to regulate to ensure that ISPs comply with codes of practice and we need to legislate to ensure there are appropriate criminal sanctions for those who create or perpetuate offensive and illegal content online.

We will listen to all arguments, read all reports and test the effectiveness of all methods to crack down on unsavoury and illegal material on the web.

Action to date
As a measure of how seriously we rate protecting families the Government introduced the Online Content Scheme in 2000 which banned X and RC (refused classification) -rated material from being hosted on web servers in Australia. R rated material operating without age-verification controls is also prohibited.

The Scheme implements strong criminal sanctions against perpetrators of child pornography and empowers the Australian Communications and Media Authority to issue fines of up to $55,000 per day for Internet Service Providers (ISPs) and content hosts that knowingly host this material.

While there have been no ISP prosecutions using the Broadcasting Services Act, more than 340 take-down notices have been issued by ACMA in relation to Australian hosted content since the scheme was introduced.

Australia can boast close to a 100 per cent success rate in cracking down on illegal and offensive content hosted by Australian ISPs as all take-down notices have been complied with.

And if ACMA is satisfied that Internet content hosted outside Australia is prohibited or likely prohibited under Australian law, Internet filters are updated to block its details.

Filters are considered the best means for a user to regulate their own Internet experience and the Government currently requires that Internet filters are offered at cost or below,/

that ISPs display Internet safety information on their web pages and regularly update their customers about how to enjoy a safer Internet experience.

The Australian Communications and Media Authority can fine ISPs up $27,500 a day for non-compliance with these industry codes.

A recent audit conducted by ACMA found a high degree of compliance with the industry codes from the largest 24 ISPs in Australia.

The audit demonstrates the effectiveness of the codes of practice which form part of the Government's Online Content Co-regulatory Scheme.

The Online Content Scheme also created the Australian Government's Internet Safety Agency – NetAlert.

Since its creation NetAlert has become a key source of information on Internet safety for Australian families.

The NetAlert Internet site has an Internet Safety Advice Centre, you can report offensive material or suspect Internet sites to ACMA, there is a safety toolkit for parents and a kids section where NetAlert mascot Netty can teach kids how to safely surf the net.

To complement these measures we have provided more than $35 million to the Australian Federal Police to set up specialised teams to protect families and children from sex criminals.

The AFP Online Sexual Exploitation Team (OCSET) was created to provide the AFP with national assessment and coordination capability for international and national referrals of child pornography.

This investment in protecting families online has reaped real rewards.

In 2004, the largest ever on-line child pornography investigation Operation Auxin resulted in the execution of 503 search warrants, the arrests of 250 people across the country and the laying of 2279 charges.

And laws introduced into Australia last year provide severe sanctions for sex crimes against children perpetrated by using the Internet.

The use of the Internet to 'groom' or procure children with the intent of engaging in sexual activity with them carries a penalty of up to 15 years jail.

These laws also carry a penalty of 10 years imprisonment for anyone who accesses or transmits child pornography online.
Australia has achieved a great deal when it comes to cracking down on hosts of inappropriate and illegal online content and the people that push it.

International actions
But we also take strong action on an international scale.

In addition to bilateral and multilateral efforts, Australia takes part in a number of international fora to better share information about online content.

Australia is an active member of the Virtual Global Taskforce which is made up of law enforcement agencies from Australia, the UK, the US and Canada - working together to fight child abuse online.

Over the past 12 months, the Taskforce has received more than 300 reports from concerned adults and children about activity online.

The Taskforce's Operation PIN – where a website purporting to contain images of child abuse was used to lure in sex offenders – resulted in the charging of 27 individuals, including three in Australia in March this year.

ACMA is also an associate member of the Internet Hotline Providers Association (INHOPE), an initiative that sees Australia work closely with members of the European community and the US to crack down on child pornography.

Australia was also recently instrumental in lobbying, along with the US, for the international registrar of domain names to refuse a proposal to establish a .xxx Internet domain.

We are of the view that the creation of a .xxx domain would lead to an increase in pornography on the Internet, act as a haven for illegal material or push offensive content on vulnerable groups.

ISP filtering

While a lot is already being done, we must continue to do more to educate parents about the pitfalls and the positives of the Internet and do more to give parents and children the tools to make their online experience safer.

There have been many voices in the Internet pornography debate, I would acknowledge the contribution of many of my colleagues and say that all are sincere.

But I fear that many of these voices are not well informed about the best available technical solutions to Internet pornography.

I support all efforts to find the best way to make the Internet a safer place and I would like to make it clear today that the Government has not and will not rule out any proven measure to protect children online.

But, whatever actions we take must be the most effective tool at our disposal.

Recently there have been ardent advocates of mandated ISP level filtering - whether through a mandated server level system or through what has been called Clean Feed.

Clean Feed is anything but clean – it does not block all pornography or other offensive sites and does not make the Internet safe.

The system – operated by British Telecom in the UK– is limited to blocking the few thousand known child exploitation sites – horrid and criminal pornography involving children.

While, on the surface this may appear a step in the right direction, there have been serious concerns raised in the UK about the effectiveness of Clean Feed.

Clean Feed does not block all pornography or other offensive sites and it does not make the Internet child safe.

Where blocking known websites at the ISP level might reduce the chances of stumbling across pornography, it does not address e-mail, peer to peer or chatroom issues.

With e-mail, children could be sent offensive content by friends or strangers;

Peer to peer networks such as BitTorrent can allow children to download entire pornographic movies from other users and are as easy to use as websites.

Pornographic material can be exchanged in chatrooms and, even more concerning, children can be approached by potential attackers.

Clean feed is not able to analyse and block websites based on more sophisticated techniques such as skin tones and as soon as a website has been identified and put on the Clean Feed list – the providers of the site just change their host to get around it.

It is also doubtful that Clean Feed could be scaled effectively to cover the whole range of pornography on the Internet.

As the chief executive of the Internet Industry Association Peter Coroneos said: ‘mandatory ISP filtering sounds like a good idea in theory, but it adds very little to the current scheme, which exceeds the protections of the clean-feed system in Britain’.

The issues with Clean Feed are symptomatic of the broader problems with filtering at the ISP level.

The Government has looked at the efficacy of ISP-level filtering three times; firstly in 1999, a CSIRO technical trial; in 2003-04 as part of the review of the Online Content Scheme; and last year during a trial conducted by NetAlert, involving RMIT and ACMA.

Each report has found significant problems with content filter products operating at the ISP-level.

I acknowledge that there is another trial of ISP filtering currently underway in Tasmania and I will consider the outcomes of that trial.

Revealingly, no advanced economy in the world has introduced mandatory server level filtering. And even where it has been introduced – in countries such as Saudi Arabia, China and Pakistan – it has proven problematic.

All these countries have experienced high levels of circumvention of these controls with industrious users using the phone system to contact an ISP in another country or using proxies to bypass the controls.

Evidence from the Saudi trials suggests that the central filtering system currently blocks a list of more than 12 million addresses, slowing Internet access by as much as half, with up to 10 per cent of sites still getting through.

And Internet users can already access step by step guides for side-stepping ISP filtering from the Internet itself.

The Australian trials have also found the effect on performance of the Internet by ISP filtering to be substantial and a lack of scalability of the filters to larger ISPs.

Any filtering mechanism needs to be both effective at blocking unwanted content as well as having a minimal impact on the performance of the network.

Like Clean Feed ISP filtering does not deal with issues related to e-mail, peer to peer or instant messaging.

It also doesn't allow the user to customise filtering levels to suit different ages or family values a Professor of Gynaecology will have very different requirements to a seven year old.

But most importantly ISP level filtering cannot not log children's activity to allow for parental monitoring.

Some argue that people who do not want ISP filtering would be able to opt out and that any success rate at blocking offensive sites is at least some progress in the fight against porn.

The reality is that Internet users who are getting large amounts of innocent material blocked are likely to be so frustrated that they opt out of filtering and leave themselves unprotected.

The other danger is promoting the notion that the Internet is now 'filtered' or 'clean' when pornography would still be relatively easy to access or the pushers of such content would find ways around the filter.

This risks creating a false sense of security and may encourage parents to abandon other methods of protecting their children.

It is not the amount of money required to implement such a system but the effectiveness of the system that is most important to the Government. That is why we support PC based filtering.

PC based filtering
It is also the most effective option that is compatible with the Government's aim to encourage greater take-up of broadband in this country.

At a time when Australian consumers are crying out for faster and faster broadband and the Government is investing $1.1 billion to deliver just that, the impact ISP level filtering would have on performance of the Internet is an important consideration.

However, the simple fact is the closer the filter is located to the end user – the greater the content it can effectively block.

A PC based filter does more than simply protect children on the web, it gives parents much more effective control over all aspects of their children's activity online.

I read an article recently where the columnist was horrified to learn what was going on in cyberspace.

Her teenage daughter had frequented a website where she could mock up a cartoon character representing herself and be picked up and taken to a quiet bedroom with a refrigerator by another male 'cartoon character'.

None of this activity would be stopped by ISP filtering but it can be stopped by a PC based filter and a vigilant and aware parent.

Some people have raised the technical difficulty of setting up and updating a filter as reasons for not supporting PC based filtering.

I acknowledge those concerns. But while the technology can seem daunting for parents – the systems are getting simpler by the day. Many of the self-install systems on the market can be set up by running a CD-Rom.

While the Government can educate, regulate and legislate to protect families, we cannot sit in your home and supervise your children using the computer.

But parents can. You wouldn't send your child out to ride their bike without a helmet, let them get into the car without putting on their seatbelt or jump into a pool if they don't know how to swim.

So why would you be content to let your child venture into cyberspace with no protection or education about the dangers?

As part of the Government's comprehensive approach to protecting families online I have under active consideration measures to improve the take-up of filtering technology in Australia.

This would be complemented by more stringent regulatory measures to ensure that ISPs are complying with requirements and bolstering NetAlert to strengthen its educational role.

But in the meantime there are measures we can take now to ensure as technology continually moves forward, we can ensure our children are protected.

Convergence
While there are many positive benefits to advancements of technology, the evolution of devices such as mobile phones or mobile TV pose challenges for Government in terms of regulating content which may be offensive or illegal.

In recognition of these issues, last year I asked my Department to undertake a review of the regulation of content delivered to convergent mobile communications devices.

The Government also directed ACMA to require appropriate restrictions to be placed on access by minors to adult content on mobile services.

Last year, a service provider determination was implemented that prohibits the supply of illegal content and requires mobile Carriage Service Providers to restrict access to content suited only to adults.

It also requires adult content provided via premium rate SMS and MMS to be carried on a restricted number range and for child safety measures to be in place for mobile chat room services.

Content Over Convergent Devices
Existing content regulation in Australia has been specific to the platform over which it is delivered (for example, television, the Internet or telephones).

The new capabilities of mobile devices to receive and display audiovisual services means that some of these platforms – and thus regulatory – distinctions are being broken down.

Mobile devices can enable access to premium voice, text and audio-visual services and, with the potential for mobile television broadcasts (using the DVB-H standard), even television content.

These developments raise the question of the way traditionally distinct content regulatory systems should apply to a single converged device.

At the very least, consumers are not likely to have an understanding that because they are using a different aspect of their mobile device to access some content (say an MMS download as opposed to surfing the web), that different content rules might apply.

The challenge for Government is to provide a regulatory framework that is sensible for both how content is accessed today and how it is likely to be accessed in the future.

The Government has explicitly recognised this challenge both in the regulatory policy underpinning communications legislation and in the terms of reference for the convergent devices review.

While the Government supports the development of innovative new communications services, these new content services may also potentially carry offensive or harmful content.

Therefore I can announce today that new safeguards will be put in place to protect consumers from inappropriate or harmful material on emerging content services such as 3G mobile phones and subscription-based Internet portals.

I will soon introduce to Parliament legislation to provide content safeguards comparable to those in place for traditional media platforms.

It will extend the current safeguards that apply to content delivered over the Internet or television to be applied to content delivered over convergent devices. This will include prohibition of content rated X18+ and above, as well as requirements for consumer advice and age-restrictions on access to content suited only to adults.

These prohibitions will be backed by strong sanctions for non-compliance with the new regulatory framework, including criminal penalties for serious offences.

These initiatives show how seriously this Government takes the issue of protecting children from inappropriate and offensive content.

Conclusion

The Government is firmly committed to keeping our children and families safe online. New technologies and the growth and pervasiveness of the Internet provide us with many opportunities to make our lives better and easier.

But we must ensure that they do not provide a pipeline for perversion into the home computer or your child's mobile phone. Because of rapid technological changes. I will not rule out any potential solution that will help parents and protect families.

The Government's approach to protecting families online is a work in progress and will not cease to look for ways to equip Australian families with the tools to crack down on the scourge of inappropriate or illegal material on the Internet.