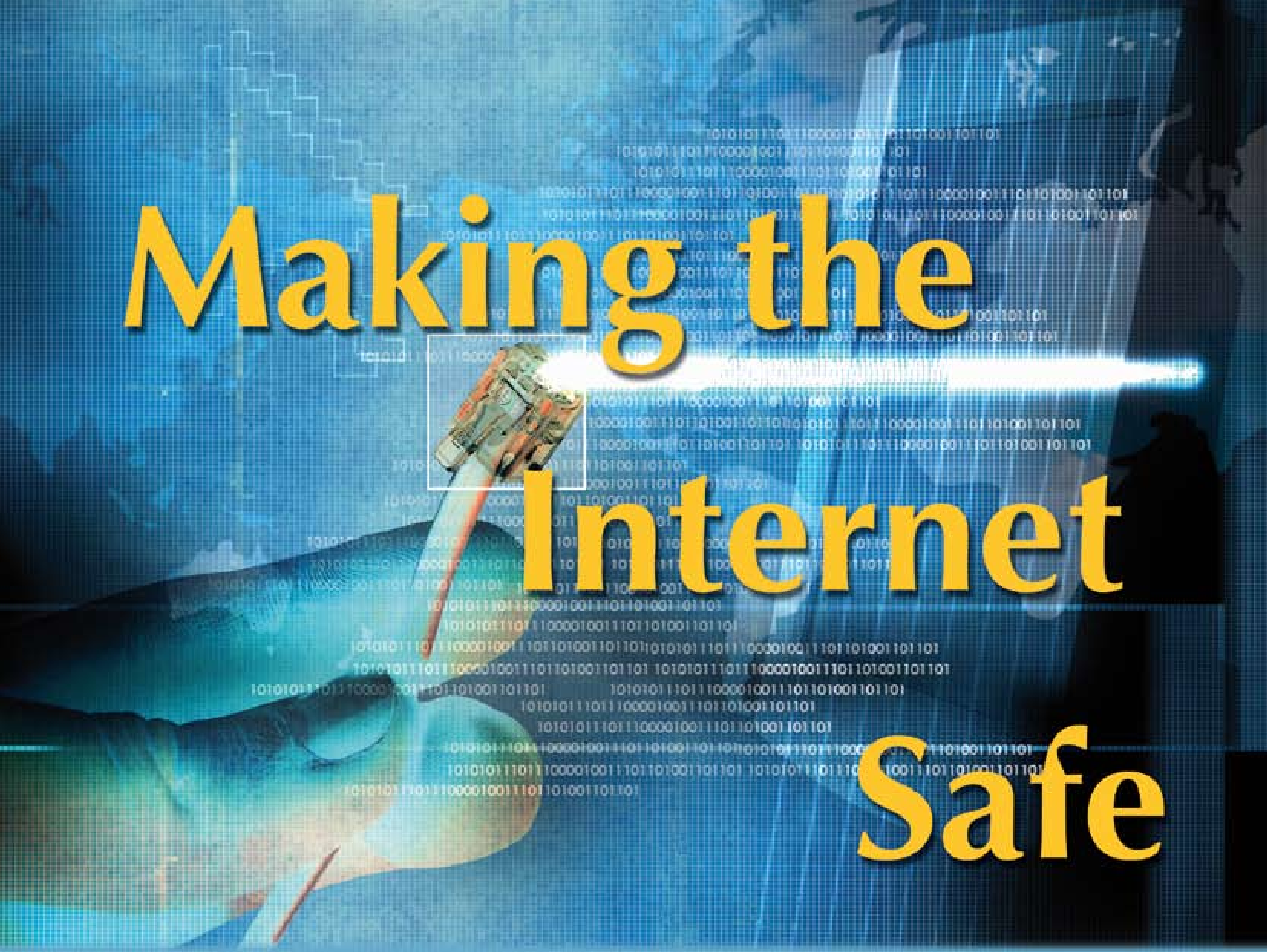


Making the Internet Safe

- Expanded blacklist filtering of illegal content
- Helping families manage the internet and mobile phones
- Fast-track promised filtering trials
- Policing of sexual predators

Australian Family Association
582 Queensberry St, North Melbourne, Vic. 3051.
Ph: (03) 9326 5757
Download copies from: www.family.org.au

POLICY ISSUES

Public concern is growing rapidly over the vast and growing array of seriously disturbing and illegal content on the internet.

There is no one "silver bullet" capable of filtering such content. However, as a matter of principle, what is illegal in other forms should also be illegal on the internet. Sites with illegal content should be shut down, or if they originate overseas, be blocked by filters.

The major thrust of Federal Government policy has been to provide free, home-based filters to families. The problem with home filters is that they are easy to bypass.

Federal Government policy has also relied on having the Australian Communications and Media Authority (ACMA) provide an official blacklist of prohibited sites for optional use to internet service-providers (ISPs) and providers of commercial filter software. The problem with the blacklist is that it registers a mere 850 sites, a very small proportion of the millions of problematic sites accessible online.

Recently the Government made it a requirement that the new free family filters use the ACMA blacklist. Unfortunately, no effective strategies have been adopted to make the ACMA blacklist more comprehensive, a major weakness of current government policy. Meanwhile some teens have already demonstrated how easy it is to bypass the government's free filters.

In contrast the community wants primary filtering to be done at the ISP level.

To this end, the government should mandate that ISPs use the ACMA blacklist. Then the blacklist needs to be greatly expanded to make it an effective filtering tool. In addition, the effectiveness of ISP-filtering using the blacklist might be enhanced by the use of new automated filtering technologies. However, the Federal Government is yet to fulfil its promise to trial such groundbreaking technologies that are already being employed by some major institutions. The NSW public education sector filters internet access for over a million computers across its networks.

This new technology involves automated content-filtering — which can scan and evaluate video, images and text — allowing large institutions to block a high proportion of illegal pornography and some other objectionable content.

Other essential internet safety policies include ongoing public education to provide families with the necessary tools to safely manage their use of the internet and mobile phones; and policing, especially to guard children and adolescents against sexual predators or other harmful exploitation.

Internet and mobile phone technologies provide enormous opportunities for enhancing the social, educational and cultural opportunities for modern families and young people. However, the ability of families to positively use the internet is being limited by the criminal and irresponsible behaviour of many thousands of people operating in cyberspace. Governments have a clear responsibility to rein in this dark side of the internet, while new technologies are increasing the Government's capacity to make the world-wide-web much safer.

The role of ACMA and ISPs in filtering

The current focus on blacklist systems for internet-filtering means that the Government has a clear role to play in providing ACMA the resources and authority required to build a comprehensive and effective filtering blacklist.

Automated content-filtering technologies have undergone substantial development in recent years, enabling large institutions to block a high proportion of illegal pornography. Such technologies may be adaptable to ISP-level filtering, but recent evaluation in this fast-developing area has been delayed by the Federal Government.

For the medium term, the objective of governments should be mandatory, comprehensive filtering by all Australian ISPs of prohibited and illegal content, using the most comprehensive technology and software available. The growing array of illegal content to be filtered includes X-rateable material, content that would be refused classification, and R-rated material that fails to provide restricted adult-only access.

While we urge the Government to fast-track evaluations of developing filtering technologies, there are other important policy changes that can make the internet safer in the interim.

1. **Urgent priority must be given to making more funds available to ACMA to comprehensively expand its filtering blacklist:**

- Recent funding improvements to ACMA are welcomed. Despite this, considerably more human and technological resources are urgently needed for identifying illegal and prohibited content, if the ACMA blacklist is to make any meaningful contribution to the filtering of the vast amount of such content on the internet.
- The continued failure of the Government to mandate that ISPs use the ACMA blacklist for filtering may reflect past inadequacies in the blacklist. However, major improvements in filtering technologies and greater public awareness of the extent of the problem have led to strong community demands for more extensive filtering, starting with a comprehensive mandated blacklist supplied to ISPs, oversighted by ACMA.
- There is a new opportunity to augment the ACMA blacklist. Some large institutions, here and overseas, are using automated content-filtering technologies to identify illegal and harmful sites for inclusion on their internal blacklists. There is a need to investigate the feasibility of ACMA obtaining this institutional data — either on a cooperative or commercial basis — for possible inclusion in a more comprehensive and meaningful ACMA blacklist.
- ACMA should also seek to identify certain legal sites that the community considers to be harmful, such as those promoting anorexia. By listing such sites on a "grey list", ACMA would be providing parents with additional filtering tools, either for their home computer or for use by ISPs.

2. **The Federal Government must give urgent priority to field-testing with commercial ISPs the most comprehensive technology and software available for large-scale internet-filtering.**

Evaluation of these trials must be made transparent and open by including community advocates of filtering, as well as government departmental and ISP representatives. Evaluation criteria must aim at filtering outcomes that are consistent with the law in other domains. Also, it must recognise the appropriate needs of children and adolescents.

If the tests are successful, the Federal Government must move to mandate comprehensive automated content-filtering of prohibited content by all Australian ISPs.

Should the ISP-filtering trials prove wanting, the Federal Government must provide significant incentives for software-development companies to advance the technology to the stage of viable, large-scale filtering. This must include the development of software capable of identifying and blocking a range of prohibited or illegal content, as well as X-rated pornography and even more extreme content. The Government should also encourage the development of technical capability to identify other sources of harmful content, such as sites that incite anorexia, bulimia and suicide. This would facilitate further effective voluntary filtering options, through tools such as "grey lists".

3. **ACMA should begin developing a code for Australian web sites to be self-rated in accordance with the national film and literature classification system, and should cooperate with other nations to develop a standard international approach to self-rating. The aim should be to allow users to choose appropriate filtering below the prohibited content level, at either the ISP level or in the home.**

Filtering by institutions and families

4. **As part of their duty of care, all public institutions — especially libraries and schools — ought to develop a national filtering code of conduct appropriate to their institution. Different levels of filtering should apply to children, teenagers and adults, based on the national film and literature classification system.**

5. **The Federal Government's $84.8 million plan to provide free home-filtering packages may be endorsed only as a necessary second-level filtering strategy.**

Education for families and children

The Federal Government has committed $33 million to fund education campaigns for parents and young people under their Protecting Australian Families Online (PAFO) initiative, through NetAlert and ACMA. Advertising and educational resource packs, together with advice and help-lines, are being made available to families under these initiatives. However, assurances are needed that this funding will be ongoing. In particular, government strategies should be family-focused. They should reflect the substantial body of research on the effectiveness of authoritative parenting styles and help involve, educate and equip parents to authoritatively guide their families to wiser and safer use of the internet.

6. **The government needs to commit to funding major ongoing education campaigns that involve the community in developing appropriate education strategies. The campaigns should target the following:**

- **Parents:** to make them aware of the dangers their children face on the internet and to give them the technical tools and personal confidence to guide their children towards safe and healthy use of these new technologies.
- **Children and teenagers:** to encourage developmentally-appropriate awareness of online and mobile phone risks, and of the role their parents can play in helping them more safely navigate the new technologies. In particular, young people should be helped to understand the growing need for them to protect their identities and personal safety in chat-rooms, instant messaging, personal web pages and blogs.
- **Employers and employees:** raising their awareness of the potential for significant productivity loss through inappropriate internet usage, which risks users becoming enmeshed in compulsive consumption of illegal content online. Employer groups should develop internet-filtering codes of practice.

Policing

7. **The Federal Government's increased funding of federal police targeting of child sex-offenders is important. However, so long as there is no mandated, comprehensive filtering of illegal child pornography, access to such content will only feed further demand for child porn. Mandated, comprehensive filtering of illegal child porn is a fundamental preventative measure in curbing the appetite for child porn, and is essential for protecting vulnerable children.**

8. **The Federal Government must cooperate with other countries to:**

- study effective filtering strategies;
- exchange blacklists of sites to be blocked;
- seek improved commitment by other nations to shutting down sites hosting illegal content and devising appropriate penalties; and
- track criminal networks carrying out illegal activities on the internet.

Mobile phone challenges

Experts are alarmed by the ease with which vindictive peers can harness mobile phone technology to bully and harass other young people. Solutions involve education and the development of filtering technologies that as yet are only in their infancy.

The Government should educate parents about the many benefits of setting limits around mobile phone use by children and adolescents. Tools and emerging technologies that enhance parental guidance, involvement and effectiveness should be welcomed and encouraged.

Strategies to help parents and young people manage phone use to minimise the risks of phone-bullying need to be explored further. There needs to be a community debate over how this technology is used by children and teens. For example, should children's mobile phones be used primarily as communication safety devices, as they were originally envisaged by most parents?

Mobile phone technology operates in three ways:

a) The latest mobile phones can access the internet, in the same way as a computer. Hence, the internet-filtering policies listed above would automatically apply to mobile phone internet use.

b) Soft and hard-core pornography can be downloaded in the form of video, photos and graphics from advertised providers by dialling up certain access numbers that are regularly advertised on late-night television.

c) Direct mobile-to-mobile phone transmission of videos, pictures and graphics. For example, a person can make a video, or download a photo, on his mobile phone and send it to the mobile phones of friends.

Currently, there is no comparable filtering technology for telephony, infrared, bluetooth, wireless and other protocols under (b) and (c), as exist for the internet protocol under (a).

9. **As part of the Federal Government's major public education campaign, parents should be encouraged to purchase mobile phones, or phone plans or other software, that restricts their children's use of phones to voice and text-messaging.**

The Government must require that telecommunication companies provide mobile phone plan options, including "white lists" that allow parents to restrict a mobile phone's use to voice and text-messaging for a limited range of telephone numbers.

10. **Content downloads from advertised sellers to mobile phones should continue to be subject to the film and literature classifications system. Providers of X-rated content, or content that has been refused classification, should continue to be prohibited. Recent laws requiring provision of tight age-restricted access, to stop under 18 year-olds accessing MA15+ and R18+ rated content, are welcomed.**

11. **Phone downloads of illegal and objectionable content originate largely from Australian sites, thereby enabling phone-carriers to easily blacklist specific phone numbers and have them blocked. Therefore, parents should have the option of choosing ratings for their children's phones, based on the ratings of the national film and literature classification system. They should have the option of having their telephone-provider filter downloads according to these ratings.**

The Federal Government should provide appropriate financial incentives for software companies to develop filtering technologies for mobile phones.

FREQUENTLY ASKED QUESTIONS

Why does the community need internet-filtering?

Governments are legally empowered to prohibit conduct that violates public safety and security, and to enforce such laws. Our criminal law also recognises incitement to commit criminal offences as a crime. Under such laws, governments:

- prohibit materials from being published that offensively depict or describe drug misuse or addiction, crime, cruelty and violence, as defined under the national film and literature classification laws;
- proscribe music, movies and images from being pirated, sold or exchanged without the payment of royalties;
- ban terrorist cells and the distribution of terrorist and bomb-making manuals;
- regulate gambling and guard against money-laundering, fraud and identity theft, a rapidly growing problem;
- prosecute illicit drug-trafficking, or human-trafficking for prostitution;
- track and prosecute sexual predators;
- restrict or prohibit access by children and adolescents to material or content that is considered harmful because of its extremely violent or pornographic nature;
- ban the sale and distribution of child pornography and other illicit material that is beyond R-rated and X-rated classifications; and
- ban the online hosting, from within Australia, of content that is X-rated, or R-rated content that has no restricted age access measures.

Governments spend tens of billions of dollars annually enforcing such laws. Yet all these illegal activities — and many, many more — are now accessible across the internet because of law-enforcement failures, or because the content is coming from sites hosted overseas.

ISPs have an ethical responsibility to use appropriate and effective tools to filter out as much of this prohibited illegal content as possible. Yet many ISPs and the internet-users' lobby have opposed mandated, comprehensive ISP-filtering.

A major problem is that, while governments have been more than willing to take a tough line on some aspects of the child pornography problem, they have virtually turned a blind eye to the millions of sites in which adult pornographers actively attempt to solicit a sexual response and return visits from children, especially male children, and teenagers.

Some content found online may not be illegal, but it is still of serious concern to many families, e.g., sites promoting suicide, or self-starvation or other forms of self-harm.

These issues establish a case for a multi-pronged approach to tackling the dangers of the internet.

Shouldn't people be able to decide what content they want to look at on the internet?

It is inconsistent to say that child pornography, violent porn, adult solicitation of children and adolescents into sexual involvement, drug-making formulas or money-laundering techniques should be illegal in all other forms except as content on the internet.

It is ludicrous to suggest that filtering of such illegal or dangerous content should be on the basis that people can "opt in" or "opt out". That is like saying, "It is against the law to drive on the left-hand side of the road, unless you choose to do otherwise." Illegal activities should remain illegal, including when undertaken on the internet.

This is where the Australian Communications and Media Authority (ACMA) guidelines on "service-provider responsibilities" are inconsistent. ACMA says, "Industry codes of practice require ISPs to take appropriate steps to protect the public from prohibited content," but then says that the filtering of prohibited content is on an "opt-in" basis. (www.acma.gov.au/WEB/STANDARD/pc=PC_90157)

Can comprehensive filtering work on a large scale with ISPs?

Many overseas ISPs already offer filtering of varying quality to users on an "opt-in" basis. Effective new technology has now been developed for institutions to filter large volumes of illegal pornography and some other illegal and objectionable content.

Large-scale filters utilised in the NSW Department of Education and Training currently do a comparison of web requests to large lists of allowed and disallowed sites. Appropriate action to block or allow the site is taken if the site is recognised on a list. If a request is not on the lists, the filter then proceeds to scan the site requested. If a site is evaluated as being undesirable, it is then added to the "disallowed" list. There is also an automated program (a web-crawler) that trawls the web proactively evaluating sites and progressively building the list of prohibited sites.

These filters also have modules that are able to scan e-mails and encrypted websites. There are also modules that ensure "safe search" programs are switched on and active on search engines (such as Google) and community sites.

It is estimated that these institutional filters may be capable of filtering out over 98 per cent of undesirable content. The process delays the system by a mere 5 milliseconds.

Unfortunately, the Federal Government has been less than enthusiastic about testing these comprehensive, automated filtering technologies for use by ISPs. Industry and other lobby groups have opposed testing or adoption of such technology on commercial and ideological grounds, arguing that unfettered flow of any content, including illegal content, is in the best interests of society. Such lobbyists have been very reluctant to acknowledge the real risks posed to children and adolescents, and society generally, by the dark side of the internet.

Doesn't ISP-filtering block people seeking to access legitimate content?

No filter can be accurate enough to always block only illegal content and never to block legal downloads. For example, filters may block an article on dismantling bombs, mistaking it for a bomb-making manual, or block medical images, mistaking them for pornography.

In the NSW government's experience of automated content-filtering, referred to above, it is estimated that only one in 12,000 legitimate sites is ever blocked by mistake. Such technologies are allowing an increasing level of sophistication in calibrating filter settings. Settings may be adjusted either to permit or to block ambiguous content. Blacklists can be used to block prohibited content that would otherwise persistently slip through the filter. As technology improves, concerns about impacts on civil liberties should be further allayed.

Will ISP-filtering affect internet speed?

Blacklists won't slow down the internet. ISPs have been happy to provide spam-filtering of e-mail, which everyone agrees has sped up the internet.

Comprehensive, automated filtering is yet to be trialled to discover how it would affect internet speed. However, blocking the high demand for bandwidth from illegal downloads would free up the internet for legitimate use. The experience of the NSW Department of Education and Training has demonstrated that filtering technology has negligible impact on internet speed at the local network level (involving approximately one million computers). Further trials at the ISP level would clarify this matter.

Will ISP-filtering be too expensive?

A 2004 Government report indicated that the initial set-up cost for ISP-filtering would be in the region of $45 million, with an annual running cost of $33 million. These indicative figures suggest that the cost to the internet industry, government and consumers would be minimal.

Don't we already have mandatory internet-filtering under ACMA?

Some politicians have claimed that Australia already has mandatory ISP-filtering, because ACMA issues a blacklist of illegal sites to ISPs and to users of the free, government-provided home-based filters. This claim is seriously misleading.

The current ACMA blacklist and other blacklists block only 850 sites, a tiny fraction of the many millions of sites hosting illegal content. The ACMA blacklist is compiled from public complaints. It does not use automated content-filtering, which is what is required to actively identify and block the huge number of sites worldwide that are hosting illegal content.

Relying on public complaints to compile a blacklist of sites is a limited and flawed process. Those who are most likely to complain about sites are the people actively trying to avoid illegal content sites in the first place! Those wanting to access illegal content are not going to report any illegal sites they find to ACMA. Further, most people are unaware of the complaints process. Others wonder about the value of reporting a few illegal sites when there are many millions of such sites on the web.

Urgent priority must be given to increasing the funding of ACMA so that it has the resources to actively search out illegal and harmful sites, e.g., sites promoting anorexia.

The government must mandate that *all* blacklisted sites be blocked by ISPs.

What is the attitude of the Coalition Government and the Labor Party to filtering?

The Coalition Government has committed a lot of taxpayers' money on this major public issue, but how effectively targetted has this been?

The Federal Government has:

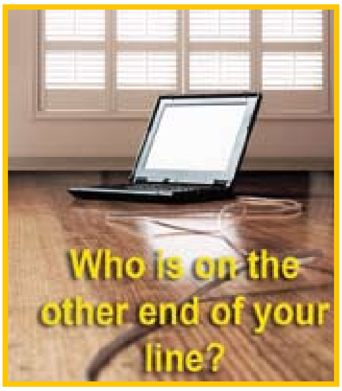
- spent big on providing home computer filters, which are relatively easy to bypass;
- funded more federal police to track and prosecute consumers of child pornography and those who solicit children on the internet. Prosecuting such offenders is important, but, so long as there are insufficient resources for ACMA to comprehensively block illegal child pornography, access to such content will only create and feed further demand for child porn; and

- moved at a snail's pace towards trialling comprehensive ISP-filtering technologies. A trial, set to start by mid-2006, never got off the ground and was recently cancelled. The Government has now promised a new trial in Tasmania, recently closing tenders for the trial's evaluation.

The Labor Opposition supports ISP-filtering in order to provide "clean feed" internet services to households, schools and public libraries. However, their policy appears to be restricted to using current ACMA blacklist filtering by ISPs. Like the Government, the Labor Opposition has not addressed the shortcomings of this blacklist. It has not indicated that it is prepared to introduce mandated, comprehensive automated content-filtering as soon as this approach is technologically feasible. Labour has also failed to indicate any intention to help fund or facilitate trials of new technology at the ISP level, or to provide incentives for research and development of such technology. Like the Government, the Opposition has not acknowledged the role that automated content-filtering could play in building the comprehensiveness of the ACMA blacklist, nor the potential to harness the current operation of this technology in public or private organisational networks.

Outstanding questions for both parties: Both the Government and the Opposition say they are moving towards ISP-filtering, but their statements have been vague, begging key questions. Will ISP-filtering be restricted to a blacklist only? How extensive will the list be, given that ACMA currently blocks only a paltry 850 sites? Or will ISP-filtering include automated content-filtering? And will ISP-filtering be mandatory, or on an "opt-in" or "opt-out" basis? In short, both Government and Opposition are yet to seriously commit to mandated, comprehensive ISP-filtering of illegal or prohibited content.

How effective is home-based filtering?



Home-based filtering can be effective if there is family awareness about dangers on the internet and about the limitations of home-filtering technology.

Just how easily a home-filter can be bypassed was made clear after the Federal Government's latest policy response. When the Government first released its free home filters in August, a 16-year-old cracked at least two of the available filters in half an hour. (*ABC News*, August 27, 2007) In media interviews, he cautioned that home-filtering by itself wouldn't be effective.

Indeed, teenagers regularly post instructions on the internet showing how to bypass the latest home filters. It becomes a challenge for teens to buck the system by getting around the latest filtering system … and letting everyone else know about it.

Consequently, many parents feel they lack the technical competence needed to ensure that their home filter won't be bypassed. They regard home filters as only a second line of defence. They want comprehensive ISP-filtering to be the first line of defence.

What role is there for public education of families on the dangers of the internet?

Internet use poses two issues for families: poor parental awareness of the dangers to which their children can be exposed; and the naiveté of children and teenagers about the dangers of sites they may access and the strangers they may meet online.

The Federal Government's internet education campaign is addressing some important areas:

- where the computer is placed in the home, and how it is used;
- how to handle internet chat-rooms, instant-messaging, blogs and personal web pages; and
- parents discussing with their children and teenagers how to handle dangers on the internet, so as to protect themselves and friends from predators, identity theft, bullying and other threats.

However, other important areas of education need to include:

- how to hold responsible discussions on the internet, in a way that positively connects people and builds relationships, and avoids online communication of scandal, harmful gossip and vilification that can hurt others, damage relationships, jeopardise future job prospects and dissolve social structures;
- how to develop a healthy lifestyle balance with time for sleep, sport, family and friends and other non-cyberspace interactions; and
- how to use the mobile phone responsibly.

Government strategies should focus on encouraging and equipping parents to positively help young people to responsibly and safely use the internet and mobile phones. Many parents are demoralised and misinformed about their real capacity to be effective guides and boundary-setters for their children and adolescents. Research shows that parents need to be authoritative, involved and loving in helping their children and adolescents to make wise choices, adopt safer practices and minimise online risks.

What role should the federal and state police play in monitoring the internet?

Policing the internet for sex-offenders is vital. There are 50,000 predators scanning the internet at any one time, according to some estimates. The extent of this problem actually underlines the need for mandatory, comprehensive ISP-filtering.

So long as there is no mandated, ISP-filtering of illegal child pornography, access to such content will only feed further demand for child porn. In addition, there are many non-child porn sites that still may foster demand for pornography involving younger and younger subjects, or more violent pornography. Pornographic genre categories such as "barely legal" may help foster tastes or compulsions that lead on to child pornography.

Can mobile phone content be filtered?

The latest mobile phones can access the internet, like a computer. Hence, the internet-filtering policies listed above should automatically apply to mobile phone internet use.

However, mobile phones can also take photos and videos, as well as download photos and videos. This data can then be communicated mobile-to-mobile. This involves the telephony, infrared, bluetooth and wireless protocols, as distinct from the internet protocol.

The Federal Government needs to provide incentives for the development of new filtering systems for other telecommunication protocols/languages used in mobile phones. These systems must be developed for both carriers (telephony and internet) and phone handsets (bluetooth, infrared, wireless, etc).