1984; Rule 29.12 *General Rules of Civil Procedure 1996*.

- NT: Section 4 *Evidence Act 1939*; Rules 1.09 and 29.12 *Supreme Court Rules*.

[9] *Cole v Elders Finance & Investment Co Ltd* [1993] 2 VR 356.

[10] *Propend Ltd v Commissioner of the Australian Federal Police* (1995) 79 A Crim R 453.

[11] *Re Griffin* (1887) NSWR 132 at 134, per Innes J; *Baker v Campbell* (1983) 153 CLR 52; (1983) 49 ALR 385; (1983) 57 ALJR 749; (1983) 14 ATR 713; (1983) 83 ATC 4606; CLR at 67 - 68, per Gibbs J; *J-Corp Pty Ltd v Australian Builders Labourers Federated Union of Workers-West Australian Branch* (1992) 110 ALR 510 at 513 - 514, per French J.

[12] *J-Corp Pty Ltd v Australian Builders Labourers Federated Union of Workers-West Australian Branch* (1992) 110 ALR 510 at 515, per French J; *R v Braham & Mason* [1976] VR 547 at 549, per Lush J.

[13] *R v Braham & Mason* [1976] VR 547.

[14] *J-Corp Pty Ltd v Australian Builders Labourers Federated Union of Workers-West Australian Branch* (1992) 110 ALR 510.

[15] *Bell v David Jones Ltd* (1948) 49 SR(NSW) 223 at 227; *Warner v Women's Hospital* [1954] VLR 410 at 421, per Sholl J; *Commissioner of Taxation (Cth) v Citibank Ltd* (1989) 20 FCR 403; 85 ALR 588 at 414-415, per Bowen CJ and Fisher J. Gibbs J in *Baker v Campbell* (1983) 153 CLR 52 at 67 - 68 reviewed the decisions in *Calcraft v Guest* [1898] 1 QB 759 and *Lord Ashburton v Pape* [1913] 2 Ch 469 but did not decide conclusively on their position in Australian. For an insightful analysis of inadvertent disclosures and its effect on the relationship between legal professional privilege and breach of confidence see: Newbold, 'Inadvertent Disclosure in Civil Proceedings' (1991) 107 LQR 99.

[16] *Hooker Corporation Ltd v Darling Harbour Authority (1987)* 9 NSWLR 538.

[17] For a discussion of available remedies, see Bell v David Jones Ltd (1948) 49 SR (NSW) 223; Ashburton v Pope [1913] 2 Ch 469; Baker v Campbell (1983) 153 CLR 52 at 68 per Gibbs CJ.

[18] *Baker v Campbell* (1983) 153 CLR 52 at 67-68 per Gibbs CJ.

[19] *Attorney General (NT) v Maurice* (1988) 161 CLR 475, which distinguished between full disclosure and a mere reference to a document.

[20] [1982] 1 NZLR 561

[21] *R v Uljee* [1982] 1 NZLR 561 at 576, per McMullin J.

[22] *Baker v Campbell* (1983) 153 CLR 52 at 65, per Gibbs J; (1983) 49 ALR 385; (1983) 57 ALJR 749; (1983) 14 ATR 713; (1983) 83 ATC 4606.

[23] Dal Pont, GE; *Lawyers' Professional Responsibility in Australia and New Zealand*; 1996; p213

[24] NSW: Rule 2 *Rules of Professional Conduct and Practice* 1995.
Qld: Para 4.02.1 *Solicitors Handbook*.
SA: Rule 9 *Professional Conduct Rules*.
Tas: Rule 11 *Rules of Practice 1994*.
Vic: *Practice Rules 1998*. See also Section 64(c) *Legal Practice Act 1996*.
WA: Rule 6 *Professional Conduct Rules*.
ACT: Para 5 *Guide to Professional Conduct and Etiquette*.
NT: Rule 9 *Professional Conduct Rules*.
See also: Rule 3 in the Australian Bar Association's *Code of Conduct* and Rule 2 of the Law Council of Australia's *Model Rules of Professional Conduct and Practice*.

[25] *Rakusen v Ellis, Munday & Clarke* [1912] 1 Ch 831 at 840, per Fletcher Moulton LJ.

[26] *Rakusen v Ellis, Munday & Clarke* [1912] 1 Ch 831 at 840, per Fletcher Moulton LJ.

[27] By virtue of the equitable doctrine of confidential information

[28] Paul McGinness, 'The Internet and privacy - some issues facing the private sector', *Computers and Law*, June 1996, p26

Restricting Access to Content—Filtering, Labelling and Education

Nick Alston, Summer Clerk, Gilbert & Tobin

In mid-1999 the Federal Government, unfettered by constitutional rights of freedom of speech, led the world in passing the *Broadcasting Services Amendment (Online Services) Act*. The stated objective of the Act is to protect children from prohibited content available over the Internet and it seeks to do so by establishing a scheme of carrier liability. The Act has been the subject of intense debate within the Internet industry with many commentators criticising the approach taken. Key criticisms raised against the Act are that it imposes liability on the wrong people and that it does not achieve its stated objective.

On 30 September this year, the Australian Senate passed a motion reflecting a range of criticisms relating to the *Online Services Act*. The motion also stated that the Senate recognised the most appropriate arrangement for the regulation of Internet content is the education of users, the empowerment of end-users and the application of appropriate end-user filtering devices.

This article provides an overview of the various schemes available to prevent access by children to inappropriate material.

PICS

The Platform for Internet Content Selection (PICS) was developed by the World Wide Web Consortium (W3). PICS is an Internet protocol which allows ratings to be transferred and understood across the Internet. The software has two components - a rating system to classify content and software that uses ratings systems to filter content. PICS enables two approaches for rating of sites: self-rating and third-party rating. Once a site is labelled in a certain way, end users are then able to block material entering their computer if the material has a rating which is not acceptable. Users are able to examine each category of rating in order to choose a preferred level of information to be received for that category. Users are effectively able to define their own ratings standards. For example, a filter can be set with a value from 0 to 4 for a number of categories. Under the RSACi scheme, there are only four categories - Violence, Nudity, Sex and Language. Under one particular scheme, the "Violence" category the rating runs from "No Violence" to "Wanton and Gratuitous Violence".

Possible inaccuracy of self-ratings as well as the vast number of sites that remain unlabelled make this system problematic. All material that is unlabelled may be blocked despite a large proportion of this material being suitable for all people. Some companies have employed persons to rate web pages. Such a task has obvious practical limitations. Some programs may also block entire directories of Web pages simply because they contain a single blocked page.

PICS has been criticised more recently as providing a method for censorship by governments - specifically the process it was set up to prevent. Governments may be able to screen out what they consider objectionable material or use ratings to achieve the same end.

Two notable rating systems that are currently in use are SafeSurf and one developed by the Recreational Software Advisory Council known as RSACi. RSACi is used as the default ratings system for Microsoft Internet Explorer. These systems enable content providers to rate their own sites. Each has different categories of ratings, and so users are likely to select the system that has categories tailored to their requirements.

POSITIVES OF THE SCHEME

Permits content rating/access to move beyond the 'blunt instrument' of pornography/not pornography to encompass different community generated categories of material.

May have incidental benefits by allowing end-users easier access to information by excluding irrelevant sites.

Permits customisation of access to content specifically tailored to the individual user's criteria of acceptable material.

NEGATIVES OF THE SCHEME

This system requires voluntary rating of content. Although many users would be willing to abide by such a scheme, it is not clear that participation of a substantial number of content providers would occur.

If access was denied to all unlabelled material, a large amount of useful material would not be accessible simply by failing to have a rating.

Sample sites:

PICS: http://www.w3.org/PICS/;

RSACi: http://www.rsac.org/homepage.asp;

SafeSurf: http://www.safesurf.com/;

APPLICATION LEVEL BLOCKING

Application level blocking is a 'black list' blocking system. It involves the blocking of a particular web page or ftp site by specifying the URL of a site to be blocked. Blocking can be applied to web pages, news groups or particular news items. The blocking is accomplished by the ISP implementing software on their server to review requests to black-listed sites. Most commonly the ISP forces its clients to access the Internet through a proxy server which performs the filtering task and delivers the page to the user if the requested URL is not on the black list.

POSITIVES OF THE SCHEME

Application level blocking provides efficiencies of scale in that it needs to be implemented at only one point in the tree of Internet connectivity (ie at one ISP, rather than at each user's premises).

Sites that have offended previously will not be made available subsequently, at least at the same URL.

NEGATIVES OF THE SCHEME

Where different port numbers are used in the hypertext URL, and the filter in the proxy server is looking for the standard port number, the page with the different port number bypasses the filter.

Sites can be renamed after blacklisting circumventing the filter.

Where material traverses an intermediate site (eg a translation service) the black list may be circumvented (as the information appears to originate from a different URL than the one requested by the user). The URL of the requested material may not be black listed while the URL of the information that is actually returned is on such a list.

The scheme requires a black list to be formulated. Prior to material being present on the black list, it remains accessible.

End users may be able to circumvent blocking by reconfiguring their proxy settings.

The black list requires third party intervention to maintain and administer the list. If the list is to be synchronised across ISP's, a process must also be established to ensure this occurs.

This scheme also blocks at a high level, meaning that all users' access will be blocked in order to prevent access by a subset of users. For example, in order to prevent access by children to content, all users are blocked. This also means the scheme does not readily lend itself to tiered blocking (eg. PG, G, MA, M15+ etc).

PACKET LEVEL BLOCKING

As a message is transferred from sender to receiver on the Internet, that message is broken into 'packets' that are independently transmitted. The packet has a header part and a payload part, the former being used by routers to get the packet to its destination.

Packet level blocking would effectively operate at Internet gateways. Packet level blocking operates by comparing the packet's source address with a supplied black list of IP addresses. This is done by routers examining the header part of the switch.

POSITIVES OF THE SCHEME

As with application level blocking, material which is on a black list becomes unable to be accessed in the same form.

NEGATIVES OF THE SCHEME

Packet level blocking is indiscriminate. Entire sites are blocked where only one page may contain offending material. A site that hosts a significant amount of content is blocked by means of one offending page and the remainder of the site becomes inaccessible.

Packet level blocking can be easily circumvented by the use of alternative IP number addresses. Routers can also be circumvented by the use of tunnelling. Tunnelling involves an IP packet contained inside another IP packet. The internal packet may be black listed, but the information will pass through a router because the wrong IP address will be examined.

Similar to application level blocking, black lists are required before material becomes blocked.

END USER FILTERING

An end-user can also use filtering software on their PC other than the PICS scheme. Products offer a range of filtering and blocking strategies. Keyword blocking, one such strategy, involves the program looking for various words and, if found, restricting access to that page or removing the word. This can lead to absurd results - a headline such as "Church condemns lesbian literature" would appear as "Church condemns literature" when seen through the filter.

Other blocking mechanisms attempt to guess the nature of the content of a page and block certain pages based on the guess. The guess is based on algorithms or rules (known as "content recognition" in industry parlance).

A role for schools and libraries has already been established in the United States. All libraries and schools who are eligible for certain subsidies are required to use filtering software to prevent juvenile access to pornographic material. In Australia more schools are using filters that can block access to offensive Web sites as pressure from parents increases.

POSITIVES OF THE SCHEME

These programs allow users to choose the level of blocking they desire.

Legitimate restrictions on one user are not imposed illegitimately on other users.

NEGATIVES OF THE SCHEME

Products that remove particular offending words without notice to the end-user can have the effect of altering the meaning or intent of a sentence.

Legitimate sites are blocked if they contain a particular word that, when used in certain contexts, may be offensive. A legitimate word that happens to have the same sequence of letters of the offending word within it, may also result in restricted access to the otherwise legitimate page - for example travel information to the English town of Scunthorpe being inaccessible.

Programs that the guess content of a page cannot be as reliable as humans or exercise the judgement that is often required in these cases.

Sample sites:

CyberSitter: http://www.cybersitter.com/;

NetNanny: http://www.netnanny.com/;

WHITE LISTS

An alternative to having sites which are blacklisted, is the establishment of what are known as clean universes or white lists. White lists as the name suggests, operate in a reverse manner to black lists. Where black lists allow access to everything except sites on the black list, white lists allow access to nothing except sites on the white list.

Such systems have been established in Australia as the demand for these safe environments increases. Once a user subscribes to the clean environment, that user's PC will automatically open up within it. The PC will not be able to access the general Internet without a password. Such a system provides a parent with a great amount of control over the material their child would view online. It is a far safer system from the point of view of the parent than one in which unreliable filtering or an arbitrary rating system governs access.

POSITIVES OF THE SCHEME

The only way to circumvent the scheme is to acquire a non white-list account.

White listing involves less processing and filtering overhead, giving faster response times.

NEGATIVES OF THE SCHEME

A great appeal of the Internet stems from the vast range of material accessible. The material available through a scheme such as this is limited to the amount of content given approval by the system's administrators. The rate of giving approval to content is outstripped by the amount of new content entering the Internet.

Sample sites:

KidzNet: http://www.kidz.net.au/;

CyberPatrol: http://www.cyberpatrol.com/; http://www.kahootz.com.au/

LABELLING PROCEDURES

Under the PICS standard, the primary objective of its development was to govern parental control. Labelling can also be used to empower a user's selection of information. This is known as 'peer collaborative' filtering. A user is directed to information tailored to their area of interest. This use is not the subject of discussion in this article although it is interesting to note that labelling can have this alternative function.

In Australia the Internet Industry Association's Code of Conduct provides that ISP's will encourage those of their users who are content providers to use appropriate labelling systems. The onus is put on the ISP's to encourage content providers to use classification schemes. This is done in conjunction with ABA standards. In the United States Congress is considering legislation to sanction a process for dealing with children's access to offensive and illegal online content. ISP's may be required to provide for no fee or a nominal fee, computer software or other filtering or blocking systems that allow the customer to prevent access to online material by minors.

EDUCATION OF USERS

A new community advisory board on Internet content was announced on 26 November in Australia. NetAlert has been set up to assist in the education process of managing access to online content.

This body will run an advisory hotline by which parents and concerned members of the public can receive information regarding ways to promote a 'safer Internet experience for children'. The education of users is imperative to achieve protection of children while filtering and labelling schemes remain underdeveloped.

CONCLUSIONS

Filtering programs and classification schemes remain technologically limited. The increasing need for parents to supervise their child's online activity will remain a useful method for ensuring the child has access to material the parent considers appropriate.

Blocking done at the ISP provides efficiencies of scale in that blocking is done at only one level, however other costs of administration and implementation of the scheme warrant consideration.

End user blocking requires a certain degree of technical skill, offers higher customisability and avoids the problem of some users having restricted access because of the requirements of others.

The development of safe environments where only specifically approved pages are accessible provides parents with an adequate means of ensuring their child will not be exposed to content they consider harmful. The amount of information made available on these sorts of systems will continue to grow, however is vastly limited in comparison to the range of information available on the Internet.

This review reveals that there are a number of competing interests that must be considered when evaluating the adequacy, effectiveness or necessity of restricting access to Internet content. Further, these interests can be in direct conflict with one another and, at the very least, are often at cross purposes. Among those interests we note the following:

- preventing children having access to inappropriate content over the Internet
- allowing access by adults over the Internet to material which may be legally acquired by them in other media
- encouraging systems to allow users to better locate information they are seeking
- minimising costs of participation and apportioning them appropriately
- maximising flexibility
- maximising parental control
- maximising internal incentives to ensure the scheme is self supporting
- minimising the need for third party administrators of schemes
- minimising barriers for useability

For example a PICS based approach where end users are empowered to take control of their Internet access provides a good fit against most of these criteria. However, PICS has been criticised for not providing parents with adequate control - ironically because children are assumed to be more Internet savvy than their parents. In order to effectively implement a system, parents would need to invest time in understanding how systems work and how to prevent their children circumventing it.

Ultimately the closer filtering is to the content consumer the more easily that filtering can be customised to the needs of that consumer without restricting the rights of others. Similarly the closer classification is to the content provider, the faster content will be classified and therefore become available through filtered services. Arguably this would also increase the accuracy of classification, although this is subject to dispute. Further when filtering and classification are located with the content consumer and producer respectively, a scheme is very well placed not only to reflect actual community standards but also to evolve with them. Conversely the further such filtering and classification are from the content consumers/producers, the more easily a scheme can be implemented, administered and policed by a regulator. Further the more easily broad based standards can be created and implemented.