THE CENSORSHIP ACT: WHAT IT MEANS FOR ISPs

David Dodunski provides an industry perspective on some of the tools available to the Internet industry to comply with the Censorship Act.

So just how does the Internet industry technically comply with the *Broadcasting Services Amendment (Online Services) Act 1999* ("**Act**")?

This article examines the filtering and removal methods that are most likely to be implemented by Internet Service Providers ("**ISPs**") and Internet Content Hosts ("**ICHs**") following enactment of the Act. It also canvasses other types of client-side filtering technologies that would be better suited to the task at hand.

According to the Act, the Australian Broadcasting Authority ("**ABA**"), has the power to:

- Instruct Australian based ICHs to remove prohibited or potentially prohibited content from their server(s) that is classified RC or X, or classified R and is not subject to a restricted access system.
- Direct Australian ISPs to take all reasonable steps to prevent end-users from accessing prohibited content hosted outside Australia.
- Require Australian ICHs to remove, and Australian ISPs to block access to, content that is similar to prohibited content.

CONTENT REMOVAL

Let us assume that the ABA has instructed an ICH to remove offensive content from its servers. This is a fairly simple task for an ICH which hosts content on its own servers. However, the proposition changes where the "host" is an ISP, which by storing content is acting as an ICH. Removal of the offensive content will depend on whether the ISP can locate the content. This process in turn depends on whether the content is "live" and the precise location has been specified by the ABA. However, no amount of detail will assist an ISP if the owner of the content has moved the content. An ISP will play "cat and mouse" with an ICH chasing content on its servers. Meanwhile, the regulatory clock (one business day to comply) keeps ticking away.

CONTENT FILTERING – ACTIONS TAKEN BY ISPS

Of much more interest are the technologies involved in content filtering. ISPs will have to initiate an active and ongoing campaign to filter end user content to meet the ABA criteria to the best of their technical and commercial abilities.

In its current state, the Act is extremely broad and does not prescribe the exact software and equipment that will be required to be used by an ISP. However, it is likely that ISPs will utilise proxy server technology as their front line of defence.

A proxy server acts as a gateway between the end user and the Internet. Proxy servers are typically implemented by an ISP to speed up traffic flow and to act as a buffer between the Internet and its network. A proxy server can track and store Internet traffic. To explain how a proxy server works let us look at the difference between connecting to the Internet with and without a proxy server.

WHAT HAPPENS WHEN YOU ARE NOT USING A PROXY SERVER?

If you decided to go to Microsoft's homepage (www.microsoft.com) and your web browser was not configured to use a proxy server, here is the path the data would travel to get to and from your computer:

Request
your computer → Internet → www.microsoft.com

Response
www.microsoft.com → Internet → your computer

WHAT HAPPENS WHEN A PROXY SERVER IS INTRODUCED?

Things happen a little differently if your connection to the Internet travels via a proxy server. If the object requested is already in the proxy server's cache, then the proxy server sends a request to the web page to check if its local copy is current. If so, the proxy returns the page to the user (considerably quicker, because it is closer to the user). If the copy of the web page located in the proxy's cache is not current or does not exist, the proxy server fetches the page, caches it, and then gives it to you.

A cache is a database that stores the location and copies of all the web sites visited by users who connect to the Internet via that proxy server. The data path is as follows:

Request
your computer → proxy server → the Internet → www.microsoft.com

Response
www.microsoft.com → the Internet → proxy server → your computer

Essentially the proxy server separates the end user from the Internet, and carries out the end user's Internet requests on behalf of such end user.

PROXY SERVER USED AS A FILTER

As the proxy server contains a database of web pages, it has the power to act as a filter. The proxy server could forward (or refuse to forward) network traffic based upon its own internal rules. These rules could include blocking of sites deemed to be offensive and the blocking of certain text strings that contain offensive words.

By using the proxy server as a filter we are in effect adding another step to the process of viewing a web page. As

outlined above, the proxy currently asks two "Yes/No" questions before delivering a web page to an end user. The questions being, do I have a copy of the web page in my cache? If so, is it current? Filtering would add a third question, namely, is it allowed?

Whilst this does not seem like a big impact on performance, the problem is that, rather than caching complete web pages, a proxy server caches web objects such as text, frames, banners and animated pictures that together form the basis of a web page. The *ninemsn* web page, for example, consists of over 15 different objects. Requesting this page from a proxy server configured to filter content would result in the proxy server executing 15 extra queries. ISPs are justly concerned that filtering will slow down web traffic. For the ISP to bring the web back up to speed, huge capital outlays must be made to purchase faster proxy servers and more money spent on running this equipment. Filtering also places an administrative cost on the ISP to ensure that sites banned by the ABA are black listed on their proxy servers. As always, all these costs will be passed onto the consumer either in terms of slow access speeds or higher Internet charges.

What I have just described is how ISPs will use proxy servers to "filter" web browsing (www). However, the Act could also apply to news groups, Internet relay chat, FTP and other Internet services, both current and emerging.

Whatever the filtering solution adopted by ISPs it is unlikely to prove 100% effective. Recent tests conducted by the Electronic Frontiers Association using Internet filtering software have indicated that whilst these filters block many questionable sites, they also inadvertently block access to non-offensive sites.

CONTENT FILTERING – CLIENT-SIDE FILTERING

First generation filtering tools such as Net Nanny and CYBER PATROL work in a way similar to a proxy server installed at the client end to monitor traffic. These tools operate from a database containing good and bad sites that have been visited and rated. They essentially block access to the bad sites or allow the user to operate only within a defined "good zone".

Despite being limited to monitoring only web content, a major setback that these tools face is the ability to keep pace with the growth of the Internet. With a new site added every 18 seconds and an estimated 20% of Internet content devoted to pornography, it is unlikely that these first generation filters will continue to be effective.

Content Rating Services

The Recreational Software Advisory Council's RSACi rating is an association of webmasters who voluntarily rate their own Internet sites for classification. This rating functions within Microsoft Internet Explorer or Netscape Navigator.

There are two main setbacks with this rating system. First, though the system is two years old, fewer than 4% of web sites currently use the RSACi standard. As a consequence, software that relies entirely on the RSACi system makes 96% of the web either not available (if the software blocks unrated sites) or not freely available to the end user without some form of blocking.

Image Based Filtering

Previously, filtering technologies were either list dependent or relied on key word searches of HTML code to block access to a site. Now, recent advances in software technology have led to the development of Image Based Filtering.

Image based filtering is now available from such products as "Eyeguard".

Using sophisticated image analysis, Eyeguard checks the images being displayed for excessive skin tones, thereby protecting the user from pornographic images. Once installed, explicit images displayed on the screen from any source will automatically be blocked.

Unlike conventional web filters that can only eliminate known pornographic sites, Eyeguard protects against the actual site content. This affords the most complete security from any pornographic sites and will complement any existing Internet security program already in operation.

Until the specifics of the industry codes contemplated by the Act have been defined, we will not know for sure what technologies will need to be implemented by ISPs or the costs involved. What we can ascertain is that the most effective means of filtering will involve a mixture of ISP based filtering using proxy servers and client level complements such as Eyeguard image filtering.

If the objective of the Act is to protect a nation's citizens from exposure to perverted and immoral material trafficked via an electronic medium, then a cooperative relationship is needed between an ISP and its end users. Realising that each individual has a differing set of moral values and what may be technically and commercially feasible to one ISP may not be to another, this cooperation is unlikely to eventuate.

If you are concerned about the nature of the material present on the Internet, I advise you not to rely 100% on your ISP for protection; take additional action and implement your own end user filtering strategies. If all this seems too difficult then simply hang up on the Internet forever.

David Dodunski is a director of Eye-T Technology (Aus) Pty Limited.