- Australian Vendors of Specialised Linux Products and Services http://www.linux.org.au/ausvendors.shtml
- Excellent Linux Search Engine http://www.google.com/
- Freely Redistributable Software in Business http://www.cyber.com.au/misc/frsbiz/

Con Zymaris (conz@cyber.com.au) is Managing Director of Cybersource Pty. Ltd. in Melbourne, Australia. He has been working with computers since 1979 and now uses Linux almost exclusively for all computer needs.

1 The Cathedral and the Bazaar, Eric S. Raymond http://sagan.earthspace.net/~esr/writings/cathedral-bazaar/cathedral-bazaar.html

2 The Open Source Definition http://www.opensource.org/osd.html

3 Caldera http://www.caldera.com/

4 Pacific High Tech http://www.turbolinux.com/

5 Red Hat http://www.redhat.com/

6 SuSe http://www.suse.com/

7 CheapBytes; Linux System Labs http://www.cheabytes.com/http://www.lsl.com.au/

8 ZDNet: The Best Windows File Server: Linux! http://www.zdnet.com/sr/stories/issue/0,4537,2196106,00.html

9 Cobalt Micro Thin Servers http://www.cobaltmicro.com/

10 Uniform Commercial Code Article 2B Revision WebSite http://www.law.uh.edu/ucc2b/

11 GNU General Public License http://www.gnu.org/copyleft/gpl.html

12 The Halloween Documents http://www.opensource.org/halloween.html

13 Cyclades http://www.cyclades.com/

14 HylaFAX Home Page http://www.hylafax.org/

15 Australian Personal Computer: Linux Pocketbook Available in most newsagents that sell Australian Personal Computer magazine

The Dawn of a New Dark Age Censorship and amendments to the Broadcasting Services Act

Brendan Scott, Gilbert & Tobin

The coming change in balance of power in the Senate has prompted some shameless initiatives by the Federal Government in relation to censorship (not the Government's preferred term "content regulation"). Suddenly this year we've seen a rush of censorship across the board and the advent of new proposals for censorship of the internet. These proposals fly in the face of technical advice received by the Government and are being rushed through with very little time for community comment. On 21 April, the Government introduced it's *Broadcasting Services Amendment (Online Services) Bill.* The Bill sets out a proposed scheme for the regulation of internet content. In short the scheme is intended to move all "objectionable" content out of Australia and to block access to such content outside Australia. The proposals are more reminiscent of censorship in, say, a totalitarian regime rather than an enlightened Western democracy.

ECONOMIC REASONS WHY THE BILL IS BAD

It doesn't take too much effort to realise that everyone pays for content they acquire. If you force someone to divest themselves of content that their users want, you force them to buy that content as their users want it. If you're a small ISP, all of a sudden you're going to find yourself having to pay to download data that you previously could provide your end users for free. If the scheme is successful, the content will still be available, just forced out of Australia. Small business ISPs will have to pay carriers for that content and those carriers will, in turn, be forced to pay foreign carriers to acquire the content. In this equation everyone on the Australian side of the ocean loses out. It also means that small ISPs are the ones who have to cushion everyone else's fall.

Forcing the content out of Australia also means that inbound traffic into Australia is increased. Australian carriers are currently forced to buy content from US carriers, but must give Australian content to the US carriers for free. One of the justifications for this is that traffic is 70:30 in the US carriers' favour (exact figures vary). Recently this ratio has been gradually improving, putting pressure on US carriers to move to a fairer interconnection regime. At an APEC conference on internet financing in Japan in March this year US carriers were at pains to justify why they shouldn't pay for other people's content. Increasing traffic inbound into Australia knocks the leg out of Australian carriers' arguments for US carriers to play fair.

Interconnection payments play a fundamental role in shaping the information economy. That the Government can contend that this regulation won't inhibit the

development of the online economy defies belief.

WHAT'S WRONG WITH THE BILL ITSELF

Without cataloguing every failure of the Bill and why (it would take far too long), we propose to give a short overview of its key failings. This is a very quick glimpse at just the worst points of the proposed scheme.

RECEIVE INCLUDES SEND

This is the hoary old chestnut from the failed 1996 SCAG proposal. That proposal ludicrously defined "send" to include "receive". The 1999 equivalent is the definition of "access". Access includes access "via push technology". That is, "receive" includes "send" and all your email suddenly qualifies you for a personal take down notice from the ABA.

"INTERNET CONTENT" INCLUDES YOUR EMAIL

"Internet content" is information that is "kept" and is accessed (or available for access) using an Internet carriage service. I'm currently keeping the email in my mailbox. That email is also "available for access" (that is, available for access by me emailing it to you) using an Internet carriage service. On this definition Internet content means all of your email.

KEPT.... KEPT???

The use of the word "kept" is apparently to exclude such content as newsgroups (see the second reading speech). However the underlying transport mechanism of the internet is the "store and forward" paradigm. Everything on the internet (including newsgroups) is "kept" in some way. Prima facie all content is caught by this definition, even if it is only kept for a short amount of time. Had "kept" been defined one would not necessarily come to this view.

ACCESS CONTROL SYSTEMS

The definition of "prohibited content" includes material rated "R" which is not subject to some means of restricting access to the material (clause 8(1)(b)). Restricted access systems can only be declared by the ABA (clause 3) – the Act does not set out any objective standards. This means that until such time as the ABA declares a specified access control system as a restricted access system, all content held in Australia rated "R" will be prohibited content under the scheme, including all material held by private individuals anywhere in Australia.

WHO'S AN INTERNET CONTENT HOST?

The act revolves around the concept of an Internet content host (ICH). An Internet content host is anyone who "hosts" Internet content in Australia. As we saw above internet content is just about anything you care to mention. Prima facie, anyone who has an email account is an internet content host and, further, all material on their computer (not just in their email file) will be subject to review because it is all "available" for "access" via an Internet carriage service (in that it can be emailed to someone). "Host", of course, is not defined. There's nothing to say that a host has to make their internet content available to the public, all they have to do is "host" the content within Australia (see clauses 20(2) and 28).

INVULNERABLE COMPLAINANTS

Complainants are not required to identify themselves when making their complaint (clause 20(3)), however the ABA is required to investigate all complaints (clause 24(1)). Further, they have the benefit of a broad indemnity against civil actions by ISPs (or anyone else) where their complaints are wrong. All they have to show is that they were made in good faith (clause 27). We note that neither truth nor "good faith" is a recognised defence to defamation (for example).

THE NOTIFY AND TAKE DOWN SCHEME

Under the Bill, if someone suspects that an internet content host (ICH) is not complying with the Act, they may complain to the ABA. The ABA must investigate that complaint and notify the complainant of the outcome (clause 24). However, the ABA is not required to notify the ICH of the fact of the complaint, the fact of an investigation or the result of the investigation. The ICH is not entitled to know who has made the complaint against them. The ABA has no restrictions on how it may conduct an investigation, however, the effect of the investigation is a notice which, if it is not complied with, has criminal sanctions applying to it.

If the ABA verifies the complaint, it issues the ICH a take down notice. However, there is nothing which restricts the ABA to the actual content set out in the complaint (clause 28(1)) nor is there anything requiring the ABA to properly identify the content. All the ABA has to do is "set out" or "describe" the content. The ABA doesn't have to inform the ICH of where the content is located or which of its users put the content there or how to find the content. In the anti-avoidance provisions the ABA can also stop the ICH from hosting "substantially similar" content (eg clause 34). While the process leading up to a take down notice implies that the notice will refer to specific content (not content described in a generic fashion) there is nothing in the anti-avoidance provisions to restrict the ABA from describing similar content generically (for example, by reference to qualities or characteristics). Arguably the anti-avoidance measures allow what minimal protections that an ICH has under the notify and take down scheme to be totally circumvented. By securing a single take down notice, other content can be restricted through use of the anti-avoidance provisions and generic descriptions of the similar content.

THE IMPOSSIBLE TASK BEFORE CONTENT HOSTS

When the ABA sends out a take down notice, an ICH must take the relevant content down within 24 hours of that notice being sent (clause 35) and must

not subsequently host that content. Given that the ABA is not required to identify where the content is located nor adequately identify the content, simply taking the content down may pose a very difficult problem for an ICH. However, keeping that content off its system is an impossibly difficult burden for an ICH to overcome. If it takes certain content down on Monday, how does it know if that content reappears somewhere else on its service on Tuesday? Internet hacker rings frequently drop contraband content into unknowing servers for their colleagues to uplift later. If the ICH is also an ISP, how does it know that its end users' emails do not contain take down content?

Despite the Government's repeated claims to the contrary, the only way for an ICH to comply with this provision is to constantly review all content on their service to determine whether it is content covered by a take down notice. The Government is requiring ICHs to monitor all of the data of all of its customers including all of their personal, private or commercially sensitive data. However, it's not just ISPs that are hit by this. It's everyone who hosts content – it's everyone who has an email account.

MAKING MISCHIEF

The opportunity for mischief under this scheme is extraordinary. Once a take down notice has been issued against an ICH that ICH will be at the mercy of any person in the world who holds a copy of the content. Merely emailing a copy of that content to the ICH will put the ICH in breach of this legislation because, on receipt, that ICH will be "hosting" the content in breach of the take down notice. Further, hosting RC or X rated content is per se in violation of the scheme. Merely emailing RC rated content to a person will put that person in breach of the scheme and open to a take down notice. Remember here that while RC includes a lot of bad stuff, RC is not just child porn. In *Rabelais* a magazine article which instructed in shoplifting was classified RC.

WHAT'S GOOD ABOUT THE BILL?

Part 9 of the Bill provides much needed protections to ISPs and content hosts against capricious State and Territory legislation. For example, it makes it clear that ISPs will not be liable under State law for content that they are not aware of. It is the only part which shows the slightest understanding of the difficulties faced by internet content hosts and ISPs. The Government would do well to drop the balance of the Bill and enact Part 9.

SUMMARY

The scheme fails on any test as a sensible approach to internet regulation. It inhibits the domestic retail market for internet services by increasing the data purchase costs of the ISPs least able to afford it. It hamstrings Australian carriers in their efforts to seek reciprocal interconnection on a fair basis with foreign carriers. It puts in place a totally unworkable administrative process to implement regulation that internet users do not want, and it casts its net so broadly as would serve quite adequately as the groundwork for a totalitarian state. It is the sort of legislation that Voltaire would have railed against at the dawn of the Age of Reason and it is just this sort of legislation that should be vigorously opposed.

This paper is available on line from the Gilbert & Tobin web site www.gtlaw.com.au.

Sites to check:

The Government's media release:

http://www.dcita.gov.au/nsapi-text/?MIval=dca_dispdoc&ID=3648

The second reading speech for the Bill:

http://www.dcita.gov.au/cgi-bin/trap.pl?path=3762

The Bill itself:

http://www.aph.gov.au/parlinfo/billsnet/9907720.doc

The CSIRO's media release on the ineffectiveness of the Government's proposals: http://www.csiro.au/news/mediarel/mr1999/mr9975.html.

Their report on blocking mechanisms is at http://www.cmis.csiro.au/projects+sectors/blocking.pdf.

The EFA's action alert:

http://www.efa.org.au/Campaigns/alert99.html

The EFA is also planning a national day of action on 28 May. For more details send a message with the subject "subscribe" to stop-censorship-request@efa.org.au