THE SHERIFF RIDES INTO TOWN: A DAY FOR REJOICING BY INNOCENT WESTERNERS

ELIZABETH HANDSLEY* BARBARA BIGGINS**

Classification of films and literature has become a settled feature of our culture and legal system. Although classification is in one sense the heir of the 'censorship' regimes that stretch back as far as anyone can remember, it is misleading to think of it in such a narrow sense. Classification is not primarily about ensuring certain material is not available for viewing or reading, though that is one of the possible outcomes. It is essentially a way of providing adults with information about the content of films, literature, and computer games, so that they can make informed choices about which material they wish to consume themselves, and to which material they wish their children to be exposed. Under the National Classification Code (a schedule to the *Classification (Films, Literature and Computer Games) Act* 1995 (Cth)) adults are totally refused access only to films and videos which:

(a) depict, express or otherwise deal with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified; or

(b) depict in a way that is likely to cause offence to a reasonable adult a minor who is, or who appears to be, under 16 (whether or not engaged in sexual activity); or

(c) promote, incite or instruct in matters of crime or violence.

The Classification Board's Guidelines elaborate:

> Films and videos will be refused classification if they appear to purposefully debase or abuse for the enjoyment of viewers, and which lack moral, artistic or other values, to the extent that they offend against generally accepted standards of morality, decency and propriety.

* Senior Lecturer in Law, Flinders University of South Australia.
** Executive Director, Young Media Australia.

Films and videos will be refused classification if they contain:

(a) depictions of child sexual abuse or any other exploitative or offensive depictions involving a person who is or who looks like a child under 16;

(b) detailed instruction in:

  (i) matters of crime or violence;

  (ii) the use of proscribed drugs;

(c) depictions of practices such as bestiality.

Films and videos will be refused classification if they contain gratuitous, exploitative or offensive depictions of:

(d) violence with a very high degree of impact or which are excessively frequent, prolonged or detailed;

(e) cruelty or real violence which are very detailed or which have a high impact;

(f) sexual violence;

(g) sexual activity accompanied by fetishes or practices which are offensive or abhorrent;

(h) incest fantasies or other fantasies which are offensive or abhorrent.

No one would wish to argue that classification is a perfect system. As in all types of legal or administrative regimes, from corporate regulation to environmental protection, there will be decisions with which reasonable people might disagree. The scope for disagreement may be heightened by the use of relatively subjective standards such as 'high impact' or 'abhorrence' (though one would be wrong to think that the classification system has a monopoly on such standards). However, it is misconceived to judge a system against a standard of perfection in the sense of expecting it to produce only decisions with which everyone agrees. If everyone agreed, there would be no need for a system. While it is useful to inquire as to whether a system is *the best that it can be*, the real question is whether the system is *better than nothing*.

It is disappointing that some people seem to be advocating just that – nothing – in response to the growth of the Internet. It is perhaps only natural for people with an interest in the Internet industry to have been experiencing a sense of exhilaration at operating on a new frontier, with few or no government constraints tailored specifically to their medium. While that feeling might be addictive, there inevitably comes a time when the law catches up to the pioneers: the sheriff rides into town. Such an event might herald a period of suppression of robust frontier activity or the end to violent lawlessness and a period of peaceful prosperity, depending at least partly on what was going on before. It is contended here that the latter metaphor is more apt in the case of the Internet. There is no doubt that the Internet has been providing children with access to material to which the law otherwise denies them access (on grounds listed under the classification legislation and guidelines). This may not amount to *violent* lawlessness – which is why the sheriff is carrying not guns but software,

warnings and fines for non-compliance – but it is unquestionably a big and growing hole in the law. The loss of frontier giddiness is a small price to pay to plug that hole.

There is no basis to argue that material generally agreed to be potentially harmful to children on films and videos, or in magazines, should not be the subject of legal attention on the Internet. On the contrary, the Internet's power and (potential) pervasiveness make it crucial to immediately begin trying to develop an effective and usable system for extending classification to it. We believe that the *Broadcasting Services Amendment (Online Services) Act* 1999 (Cth) ("*Online Services Act*") represents a useful first step in that direction.

In our view, the *size* of that step is beside the point. However, it is worth commenting on the apparent concern that the Internet industry will be stifled by the need to comply with the legislation. A close look at the *Online Services Act* reveals that industry members will receive considerable guidance from the Australian Broadcasting Authority ("ABA"). There are no sanctions without notices first being issued as to the steps to be taken, and there is a likelihood of follow-up warnings.[1] Moreover, the regime is essentially one of self-regulation, with standards being set by the registration of industry codes of practice.[2] Thus, it could be said that the Internet industry benefits from the best of both worlds: writing its own rules (within certain limits), and yet having to take little initiative to ensure its compliance with those rules. If you imagine yourself as a parent first allowing your children to determine when their own bed time is, and then still having responsibility for cajoling them into bed at that time each night, and you begin to get a picture of the respective positions of the ABA and the Internet industry under the legislation.

It may be too early to predict precisely what the content of the codes of practice will be. However, the codes registered by the ABA to date, which cover only the bare minimum required by the Act, provide a foretaste of future developments. These codes address only the very basics of the regulatory regime: the responsibilities of Internet service providers ("ISPs") and Internet content hosts ("ICHs"), in relation to Australian and overseas-originated potentially offensive materials; and the obligations of ISPs and ICHs to advise customers of the availability of filtering and blocking devices. None of the other code areas, such as privacy and protections for children in relation to advertising (which were included in the version of the Internet Industry Association's code that went out for public consultation), have yet been included in the approved codes. While we are hopeful that these matters will be covered by further codes, the notion of an industry labouring under impossible burdens still appears some way off.

As debate has progressed over recent months, the more common criticism of the *Online Services Act* has been that it will be ineffective. This is essentially an argument about the size of the step that the legislation represents, which we have

1 *Broadcasting Services Act* 1992 (Cth), Schedule 5 (as amended by the *Online Services Act*), especially ss 30 (take-down notices), 40 (access prevention notices), 66 (directions to comply with code), 83 (remedial directions) and 84 (formal warnings).

2 *Ibid*, especially ss 59, 60 and 62.

already contended is beside the point. Further, it is an argument that is evidently weakened when applied to analogous contexts, such as property law. Consider the following proposition: because property is still stolen, we should not have a law against theft. Such a suggestion is clearly nonsensical. A large part of the value of the law is its persuasive deterrent force: we do not expect that thefts will never occur, but we can probably agree that there would be more thefts if there were no law against it. Most of us would refrain from purloining the property of others on moral grounds in any event, but it is fanciful to suggest that no one is persuaded by the prospect of punishment to stifle a larcenous urge. This is so despite the reality that many thieves are never caught, or never convicted. It is impossible to be sure for the moment exactly how the *Online Services Act* will work, not just because of technological uncertainty but because of the difficulty of predicting its psychological and sociological impact. However, we can be certain that it will make it *harder* for children to access unsuitable material, and therefore the number of such 'hits' will decrease. Such an effect cannot be regarded as anything but salutary. The existence of the legislation might also spread the message that the material in question is in fact unsuitable, and lead community attitudes in that regard – just as a law against theft can lead people to believe that theft is wrong. Perhaps a better analogy here would be laws against providing alcohol to children. Most adults would not provide alcohol to a child, even if sure that he or she would not be caught, because they believe that it is wrong to do so. Part of the reason that they believe that it is wrong is that it is illegal. The technical effectiveness of the legislation is therefore somewhat extraneous to any assessment of its value.

Rather than emphasising the interests of the industry or holding the legislation up to some misleading standard of effectiveness, we take as our starting point the proposition that a significant measure of the Internet's value is in its ability to avoid harming children. Just as the prosperity of Victorian England does not justify the use of child labour in the coal mines, the benefits of the Internet are at best illusory if they can be gained only at the expense of children's healthy development. Therefore, it is contradictory to say that measures to protect children derogate from the benefits of the Internet; any benefit dependent on exposing children to risk is not a benefit at all.

Parents and caregivers have an important role to play in guiding and supervising their children's use of the Internet.[3] Therefore, it is crucial that the legislation address any difficulties parents and caregivers might experience in taking advantage of the new system. In this respect, we applaud the establishment of NetAlert, a community advisory body described in the Minister's announcement as having the functions:

3 This is why Young Media Australia has developed the CyberSafety programme.

> to monitor material, operate a 'hotline' to receive complaints about illegal material and pass this information to the ABA and police authorities, and advise the public about options such as filtering software that are available to address concerns about online content.[4]

If NetAlert comes to terms with the role that it has to play in getting some real gains from the legislation for the community, its establishment will prove extremely valuable in creating and maintaining an active community presence in the regulatory scheme. It is unfortunate, however, that the body is not spelled out in the legislation. It has been set up directly by the Government, as an instance of executive action, without supporting legislation. It would have been better, in our view, if these measures had been contained in the *Online Services Act* itself, as that would have underlined their importance and their integral relationship with the other mechanisms of the scheme. It would also have made it more difficult for this or future governments to cut funding to the services in question.

These issues take on more urgency when one considers the risk, identified by Jon Casimir in the *Sydney Morning Herald*,[5] that decision-makers and citizens will use the existence of the legislation as the basis for an assumption that the Internet is now 'safe' for children. To the extent that this happens, there is a real danger that the regime could actually make the Internet *less* safe, particularly if the pundits are correct in their assertions that the effectiveness of the regime will be limited. The *Online Services Act* is not a substitute for responsible adult supervision and it does not remove the need for parents and caregivers to talk with their children about the material they locate on the Internet. To return to the theft analogy, no sensible person would refuse to install a burglar alarm just because burglary is illegal. NetAlert has an essential role to play in encouraging the maintenance of the necessary vigilance.

A final issue we have identified relates to the civil immunity provision. The *Online Services Act* will grant immunity from civil proceedings for actions done "in compliance with" the following aspects of the regulatory scheme:

- any code or standard that deals with procedures to be followed by service providers in dealing with notified content;
- the rules requiring compliance with access-prevention notices; and
- the rules requiring compliance with take-down notices.[6]

Some readers may be aware of developments in the USA, where the bulk of the *Communications Decency Act* 1996 (USA) was ruled unconstitutional by the Supreme Court, but the civil immunity provision was preserved.[7] The result,

---

4 Senator Richard Alston, Minister for Communications, Information Technology and the Arts, "Regulation of Objectionable Online Material", Fact Sheet, 10 May 1999, available at <http://www.dcita.gov.au/text_welcome.html>.

5 J Casimir, "Act of Stupidity" *Sydney Morning Herald (Icon)*, 17 July 1999, p 11.

6 Note 1 *supra*, s 88.

7 *Reno v American Civil Liberties Union* 117 S Ct 2329 (1997).

following *Zeran v America Online Inc*,[8] has been that it is impossible to sue a content provider for defamation on the Internet in that country.

The relevant section of the *Communications Decency Act* states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".[9] Of the USA provision, Wilkinson CJ of the US District Court (4th Circuit) commented:

> By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions – such as deciding whether to publish, withdraw, postpone or alter content – are barred.
>
> The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.[10]

Consequently, Mr Zeran was left without any remedy for a serious defamation posted on an American Online Inc ("AOL") noticeboard, because AOL was immune both from suit and from any requirement to divulge the source of the posting.

The wording of the USA provision stands in marked contrast to that of the Australian provision, which both goes further than and stops short of the American provision. The Australian legislation mentions "immunity", whereas the USA provision does not. However, the Australian provision also uses the term "in compliance with" to signal its primary concern with the enforcement of the legislation. Therefore, the *Online Services Act* evidences no legislative intent, such as that referred to by Wilkinson CJ, to safeguard "freedom of speech". Rather, the intent seems to have been merely to protect ISPs and ICHs in relation to their actions in complying with the provisions of the legislation, most probably in an attempt to increase the likelihood of compliance by removing a source of temptation not to comply. Both provisions could be seen as a kind of 'sop' to ISPs and ICHs who might otherwise have objected even more strenuously to the regulatory regime, but the emphasis is quite different. Whereas the USA provision actually *removes* liability to which ISPs and ICHs would otherwise be subject to, the Australian legislation merely reassures them that under the new laws they will not be exposed to *additional* liability. It is not surprising that concern about liability has been played out in the USA in terms of

8 *Zeran v America Online Inc* 129 F3d 327 (4th Cir 1997).

9 Section 230(c)(1).

10 Note 8 *supra*, at 330.

freedom of speech, given the centrality of that concept to legal and media culture in that country. However, the concept does not translate easily into Australian law, and the emphasis in the legislation here is clearly aimed at encouraging (and possibly rewarding) compliance, rather than protecting a cherished freedom. We believe that these differences support the conclusion that the *Online Services Act* will not leave potential defamation plaintiffs without remedies.[11]

The same conclusion is reached by considering the term "in compliance with" in the Australian provision. There are two ways of interpreting the term. First, it might have the relatively narrow meaning of "in order to comply with". Under such an interpretation, the immunity would extend to actions *required by* the code, standard, or rule in question, but not to all actions that happen to be in compliance. Or second, the term "in compliance with" might have the broader meaning that, as long as the ISP or ICH is complying with the relevant rules, there can be no proceedings against it for anything it does in its capacity as a provider or host.

We believe that the first interpretation is the correct one. The second interpretation is simply too broad, going far beyond the policy goals which prompted the development of the legislation. For example, it is difficult to imagine that an ISP would be immune from an action for allowing access to defamatory material simply because there was no access-prevention notice in force relating to that material. The *Online Services Act* is not about defamatory material; it is about material that is unsuitable for children.

The type of situation which the legislature more likely had in mind is one where an author has an agreement with an ISP to disseminate certain information, and the ABA issues an access-prevention notice in relation to that information. The author has no right to proceed against the provider for breach of the agreement in such a circumstance, because the notice takes precedence over the author's rights under that agreement. In other words, the immunity provisions are best understood as limited in their effect to actions relevant to the subject matter of the legislation. Given the ease with which the legislature could have adopted wording clearly conveying the broader meaning of "in compliance with", it is unlikely that an Australian court would interpret this ambiguous provision in a way that deprives people of their common law or other rights.

Overall, the *Online Services Act* is to be applauded. It represents a serious attempt to address the availability to children of material on the Internet that the Australian community has already decided should not be readily available to children. In our view, it is indisputable that the need for a sheriff at the frontier is at least as great as it is in the settled areas. Nevertheless, there is a real risk that the voices of the 'gun-slingers' will drown out those who simply want to get on with farming the land. We hope that the sheriff will be a wise and benign one,

11 Defamation plaintiffs are remediless not just against ISPs but also against the original source of any communication. This is because ISPs share with newspapers and other types of media a constitutionally based exemption from any requirement to disclose the sources of the information they publish. Although the situation of an ISP hosting a bulletin board is clearly distinguishable from that of a newspaper publishing news, freedom of speech effectively has two bites at the cherry of the plaintiff's reputation: first, to immunise the ISP; and second, to protect the source.

and would fully support action if he or she turns out to be corrupt and/or incompetent. However, the proper course now is for the pioneers to let the sheriff get on with the job and show us what can be done.