SAFELY OUT OF SIGHT: THE IMPACT OF THE NEW ONLINE CONTENT LEGISLATION ON DEFAMATION LAW

JULIE EISENBERG*

The new framework for dealing with "offensive" content created by the *Broadcasting Services Amendment (Online Services) Act* 1999 (Cth) ("*Online Services Act*") has a surprising impact beyond censorship and classification. The *Online Services Act* has an apparently unintended, but significant side effect: a new defamation defence for Internet content hosts ("ICHs") and Internet service providers ("ISPs").

One of the key motivations of the legislation has been the task of defining and delineating responsibility for Internet content. In the lead up to its enactment, a major concern of those providing or hosting Internet services was the prospect of being liable for carrying or hosting material of which they were not aware. The new regulatory scheme resolves this issue by establishing a complaints driven framework for removing content, eliminating the spectre of strict liability for carrying "prohibited"[1] or "potentially prohibited content".[2] The two entities caught by the legislation – ICHs and ISPs[3] – are not obliged to actively monitor content. They are only required to remove content following formal notification by the Australian Broadcasting Authority ("ABA"). Content filtering is dealt with at industry level in codes of practice, three of which were registered with the ABA in December 1999.

I. SECTION 91 – IMMUNITY FOR ISPS AND ICHS

Consistently with the complaints driven approach created by the *Online Services Act*, ISPs and ICHs are granted certain immunities. Schedule 5, s 91 of the *Broadcasting Services Act* 1992 (Cth), as amended by the *Online Services*

* Media lawyer and commentator, Communications Law Centre, Sydney.

1 As defined in the *Broadcasting Services Act* 1992 (Cth), Schedule 5, s 10 (as amended by the *Online Services Act*).

2 *Ibid*, s 11.

3 *Ibid*, s 3.

Act, says that a law of a State or Territory, or a rule of common law or equity, has *no effect*, to the extent to which it would:

- *subject* an ICH or ISP to civil or criminal liability for hosting or carrying content where it was not aware of its nature; and
- *require* an ICH or ISP to monitor, make enquiries about or keep records of content which it hosts or carries.

The section applies only to State and Territory laws or rules of common law and equity, leaving open the ability of the Commonwealth Parliament to require monitoring or impose strict liability for ISP/ICH conduct in other contexts.

When considering the impact of s 91(1) on non-Commonwealth laws, it is significant that immunity is broadly stated: there is no apparent limitation on the subject matter of the laws which might be overridden by s 91(1), nor is there a limitation on the type of content applicable. It does not just apply to "prohibited content" or "potential prohibited content", as those terms are used in the Act, and it does not expressly refer to the proposed cooperative State/Territory online content classification scheme.[4] Even if its interpretation could be limited by its context – the regulation of "offensive" online content – it should still apply where the outcome is broadly consistent with the stated objectives of the legislation. These include encouraging the development of Internet technologies and services, and avoiding placing unnecessary administrative and financial burdens on ISPs and ICHs.[5]

While the new defence applies to a range of State based content liability laws, such as content classification, sub judice contempt and statutory court reporting restrictions, this article focuses on its impact on defamation law.

II. ISP/ICH LIABILITY FOR ONLINE DEFAMATION

Defamation law is one of the most significant and costly areas of potential liability under State/Territory law. While there has been no decided Australian case on ISP/ICH defamation liability, a Melbourne ISP reportedly paid $10 000 to settle an online defamation claim brought against it in an English court.[6] In view of the enormous legal fees involved in defending a defamation case, the ISP appears to have got off relatively lightly. The volume of material carried over

4 The draft model online services amendment to the Classification (Publications, Films and Computer Games) Acts is yet to be finalised. In its current incarnation, it catches anyone *knowingly* or *recklessly* involved in the dissemination of "objectionable matter" online. Section 3 provides that a person is not guilty of an offence by reason only that they own, control or manage an online service, or "facilitate access to or from an on-line service by means of transmission, down loading, intermediate storage, access software or similar capabilities". This is broad enough to quarantine ISPs who provide gateways into the Internet and possibly also ICHs who have linked to another site unaware that it contained objectionable material. However, it is not broad enough to help those who have been *reckless* in giving access. The new Schedule 5, s 91(1) of the *Broadcasting Services Act* 1992 (Cth) will override this, protecting 'reckless' ISPs and ICHs who can show that they did not know they were carrying or hosting objectionable content.

5 *Broadcasting Services Act* 1992 (Cth), Schedule 1, s 4(3) (as amended by the *Online Services Act*).

6 D Passey, "Internet Provider pays $10,000 over libel" *Sydney Morning Herald*, 14 March 1998, p 18.

Internet services or posted on bulletin boards daily means that ISPs and ICHs face high volume and high value risks of being found liable for content they carry or host.

Section 91(1) is broad enough to provide a defence to State/Territory laws and common law rules that might otherwise impose liability on ISPs and ICHs for unwittingly carrying defamatory material. If so, it is wider than the defence available at common law or under the Queensland and Tasmanian defamation Codes.[7]

There seems to be little constitutional impediment to s 91 overriding State and Territory defamation laws. Although the regulation of content largely falls outside the Commonwealth's express powers under the Constitution, the *Online Services Act* only purports to regulate the position of two classes of content carriers: ISPs and ICHs. Its impact on defamation law is confined to the conduct of those entities in their use of online services. Following the broad interpretation of s 51(v) of the Constitution in *Jones v Commonwealth (No 2)*,[8] this appears to be well within the Commonwealth's power.

III. INNOCENT DISSEMINATION DEFENCES AT COMMON LAW

Publishers are generally strictly liable for disseminating defamatory material. However, the defence of innocent dissemination is available to those involved in a publication who are, first, *subordinate* distributors, rather than *primary* publishers; and second, able to demonstrate that:

- they did not know of the defamatory content of the publication;
- this ignorance was not due to their negligence; and
- they had no grounds for supposing that the publication was likely to contain defamatory matter.[9]

This defence has traditionally protected disseminators such as newspaper vendors and libraries. The High Court's statements in *Thompson v Australian Capital Television Pty Ltd* suggest that the defence may also be open to ISPs or ICHs: "[t]here is no reason why in principle a mere distributor of electronic material would not be able to rely upon the defence of innocent dissemination if the circumstances so permit".[10]

Proving that the right circumstances exist will not be simple. In *Thompson*, a broadcaster which retransmitted another network's program was found *not* to be a subordinate distributor because it chose (but was not bound) to run an instantaneous relay transmission of a live current affairs program knowing of the

7 *Defamation Act* 1889 (Qld); *Defamation Act* 1957 (Tas).

8 (1965) 112 CLR 206.

9 *Emmens v Pottle* (1885) 16 QBD 354, cited in *Thompson v Australian Capital Television Pty Ltd* (1996) 71 ALJR 131.

10 (1996) 71 ALJR 131 at 135.

risk of defamatory content. The High Court considered it a "primary publisher" because it retained the ability to control and supervise the broadcast.

Similar issues are relevant to whether ISPs and ICHs could be regarded as "subordinate distributors". Early analogous USA cases give limited guidance. In *Cubby v Compuserve*,[11] the large number of publications on Compuserve's electronic database and the speed with which they were uploaded were factors in finding that the ISP was a distributor rather than publisher of its bulletin boards. In *Stratton-Oakmont v Prodigy*,[12] the self professed 'family friendly' Prodigy was treated as a primary publisher because it applied editorial control over the content of messages on its bulletin boards, including screening software and a manual scanning of notices by employees.

Applying this distinction to an Australian context leaves ISPs in an uncertain position. By monitoring or screening content, ISPs risk losing their "subordinate distributor" status. If they do not monitor, but have "grounds for supposing" that some of their services contain defamatory material, they will fail the "innocent disseminator" test.

The options faced by ISPs are further complicated by their *Online Services Act* obligations. The Division 3 scheme encourages development of industry self regulatory codes. The ABA is empowered to make standards where the codes fail to deal with specified issues,[13] such as giving customers the option of a "filtered Internet carriage service".

Filtering can occur at user level or ISP level. The current codes of practice provide for ISP obligations to be met by handing out software to users, preserving the position of an ISP as "subordinate distributor" of Internet content. But if filtering is offered at ISP level (whether now or under future regulatory requirements), the impact will vary depending on the type of software used. Many current filtering technologies use keywords to block prohibited sites. Others offer software with an 'opt-in' capacity; that is, they rely on manual screening to create a list of acceptable sites.

The process of screening for illegal or offensive content involves very different considerations to vetting defamatory content and assessing whether defamatory content is defensible. Content filters are not 'Defamation Net Nannies'. Nevertheless, the analogous American cases and *Thompson* suggest that, in deciding whether an ISP or ICH is a "primary publisher", courts in defamation cases will need to be convinced that filtering technologies used at ISP/ICH level do not amount to a type of editorial control. The only certain outcome for an ISP/ICH will be the expense and complexity of proving "subordinate distributor" status to the satisfaction of a court.

In contrast to the common law position, the s 91(1) immunity has the potential to provide a uniform and certain approach for ISPs and ICHs not directly involved in creating or vetting content they disseminate.

---

11 776 Fsupp 135 (SDNY 1991).

12 [1995] NY MiscLexis 229.

13 *Broadcasting Services Act* 1992 (Cth), Schedule 5, ss 68-71 (as amended by the *Online Services Act*).

IV. IMMUNITY FOR ISPS/ICHS – INTERNATIONAL COMPARISONS

Section 91 immunity is broadly in line with international approaches. The most liberal provision is found in s 230 of the *Communications Decency Act* 1996 (USA). It says that "[n]o provider or user of an interactive computer service shall be treated as publisher or speaker of any information provided by another information content provider". Part of its policy justification was to encourage ISPs to block and screen materials without fear of being found to be strictly liable as publishers of that material. The court in *Zeran v America Online*[14] confirmed the breadth of s 230 by allowing an ISP to escape liability for hosting disparaging content, even after being notified of the problem.

The UK Government took a narrower approach in its *Defamation Act* 1996. Section 1 provides a defence for "the operator of or provider of access to a communications system by means of which the [defamatory] statement is transmitted, or made available, by a person over whom he has no effective control" provided the person "took reasonable care and did not know... he contributed to the publication of a defamatory statement".

In *Godfrey v Demon Internet Ltd*,[15] the English High Court considered the position of an ISP which carried a bulletin board containing defamatory comments about the plaintiff. The High Court rejected Demon's threshold argument that, as an ISP, it was not a publisher in the first place, finding that ISPs were clearly primary publishers.[16] The s 1 defence was not available once Demon had been notified of the defamatory posting and failed to remove it.[17]

Section 91(1) falls somewhere in between these two approaches. It removes from ISPs and ICHs any obligation to screen for defamatory content and protects them from liability if they are filtering content for other purposes but are unaware of defamatory content. It goes further than the English provision

---

14 [1997] 129 F3d 327. See also *Blumenthal v Drudge* (US District Court, District of Columbia, Case Number, 97 CV-1968). The ISP, American Online ("AOL"), had entered into an exclusive agreement to pay Matt Drudge to publish the Drudge Report (which had originally exposed the Clinton/Lewinsky affair) on its service. AOL had publicised the Report's "gossip and rumour" content as a drawcard for new AOL subscribers. Although AOL reserved the right to remove content that breached its standard terms, the Court held that it was "immunized" by ss 230(c)(1), which did not distinguish publisher and distributor liability, and 230(c)(2), which specifically contemplated that filtering or removing objectionable material would not forfeit the immunity.

15 Unreported, High Court of Justice, Queens Bench Division, Morland J, 26 March 1999, available at <www.courtservice.gov.uk/godfrey2.htm> at 26 March 1999 (Copy on file with author). See also *Godfrey v Demon Internet Ltd* (unreported, High Court of Justice, Queens Bench Division, Morland J, 23 April 1999, available at <www.courtservice.gov.uk/godfrey3.htm> at 23 April 1999 (Copy on file with author). This is a related decision on the impact of Internet customary practice on pleading a defamation case.

16 Demon relied on a USA court's finding in *Lunney v Prodigy Services* [1998] WL 999836 (NYAD 2 Dept) that, at common law, the ISP was not a publisher in a case where a "practical joker" had used someone else's identity to send a disparaging email on Prodigy's service and post it on a Prodigy bulletin board. However, Morland J said the same facts would have a different outcome under English law. *Ibid*, para 49.

17 The plaintiff only sued for the publication *after* that date, ostensibly because s1 protected Demon as long as it was unaware of the message.

because Australian ISPs and ICHs do not have to show that they took "reasonable care".

V. A UNIFORM DEFAMATION LAW FOR ISPS AND ICHS?

Last year, Attorney-General Darryl Williams called for a "fresh approach" to uniform defamation laws, after the States and Territories had yet again failed to agree on the road to reform.[18] Despite having a national media and a rapidly growing local Internet media, Australia retains an absurdly diverse collection of state based defamation laws. With the Australian Capital Territory introducing a new Defamation Bill in December 1999,[19] the prospects for uniformity get even bleaker.

Although s 91(1) presents an opportunity to clarify an uncertain area of the law, this can be easily lost. Section 91(2) allows the Minister to declare that specified State or Territory laws or rules of common law or equity are exempt from the operation of s 91(1). This curiously framed sub-section leaves a very significant issue in the discretion of the Minister: the position of ISPs and ICHs under a range of State laws and, in particular, their defamation liability. However, unless and until a Ministerial declaration under s 91(2) is issued to exclude the operation of the section in relation to defamation laws, s 91(1) appears to provide a clear, certain defamation defence to ISPs and ICHs.

The legislation did not expressly set out to achieve this goal. However, this outcome is not inconsistent with the *Online Services Act's* broad policy intention of encouraging the development of Internet services and avoiding unnecessary burdens on those who provide gateways into the Internet or facilities for large volumes of users. At the very least, the new Act provides a novel and surprisingly painless approach to creating uniform defamation laws.

18 "Disappointment at Lack of Action on Defamation", Media Release, 17 April 1998.
19 Defamation Bill 1999 (ACT).