Flamers, Trolls and Bloggers – Are ISPs and webhosts at risk from online anarchy?

*Richard Potter, Phillips Fox**

Richard Potter is a partner with Phillips Fox in Sydney, specialising in defamation and media law.

In a recent newspaper interview, the psychological profile of a 'troll' was revealed to all:

> *"I can say something nasty because I don't have to look at you, it's easier for me to be hurtful and it still serves my purpose which is to make what you're doing look silly and make me feel better about myself"*[1]

So there it is, the perfect medium for the insecure, the shy or even your everyday social terrorist.

The opportunity for a person with no other infrastructure than a computer and a telephone line to reach a mass audience and perhaps cause havoc has never been greater. Who are these strangely named beings and, more importantly, what are the legal consequences of their activities?

Terminology

Flaming is fostered by the anonymity offered by the internet. It involves venting one's anger towards another participant in a discussion group. There is a net etiquette guide called 'netiquette' which encourages the practice and requests flamers to:

> *"consider the art of flaming before pulling out the flame thrower. Any wannabe with an email can ignite a firestorm of ill conceived and boring flames. It takes diligence and creativity to pull off an artful flame. Who knows, if your flame is good enough, you might even make it into the Hall of Flame."*[2]

If a person is defamed by a 'flame', the perpetrator may well be impossible to identify. However, flaming may expose ISPs and internet content hosts (ICH's) to actions for defamation by the flamer's victim.

Trolls are another type of cyber prankster. Their activities are a little more subtle than those of the flamer. Trolls seek to disrupt online discussion groups, not by a flame throwing but by carefully provoking the discussion group into responding to controversial comments which are tailored to be diametrically opposite to the majority view of the group.

> *"Trolling is a game about identity deception, albeit one that is played without the consent of most of the players. The troll attempts to pass as a legitimate participant, sharing the group's common interests and concerns; the newsgroups members, if they are cognizant of trolls and other identity deceptions, attempt to both distinguish real from trolling postings and, upon judging a poster a troll, make the offending poster leave the group. Their success at the former depends on how well they – and the troll – understand identity cues; their success at the latter depends on whether the troll's enjoyment is sufficiently diminished or outweighed by the costs imposed by the group.*
>
> *Trolls can be costly in several ways. A troll can disrupt the discussion on a newsgroup, disseminate bad advice, and damage the feeling of trust in the newsgroup community. Furthermore, in a group that has become sensitized to trolling – where the rate of deception is high – many honestly naive questions may be quickly rejected as trollings. This can be quite off-putting to the new user who upon venturing a first posting is immediately bombarded with angry accusations. Even if the accusation is unfounded, being branded a troll is quite damaging to one's online reputation."*[3]

Again, easy to see where all this may end up, someone ultimately defamed as the debate spirals downwards into abuse. On its own, abuse is not defamatory as no one actually thinks less of a person simply because they have been abused. However, accusations can be levelled at a person which may well be defamatory, fuelled by the anger created by the troll's destructive intentions.

The practice of 'blogging' is not in itself a recent development but is increasingly entering the public consciousness. The term 'blog' is short for weblog which is a net diary with periodic entries, usually developed and maintained by a single author. The practice was started by net enthusiasts who collected and posted links to other sites on the net they found interesting. Bloggers then began reading each other's blogs, adding commentary and posting regularly. Paradoxically, blogging is therefore a personalised but ultimately communal format.[4]

By their very nature, flamers and trolls and possibly also bloggers protect their anonymity to be able to cause damage from a safe hiding place. Such individuals may be elusive to track down leaving the ISP and/or ICH in the firing line.

Where material is published on the net, the 'publisher' can also be anyone who takes part in the publication or republication of the material including the ISP or ICH. In most cases, the easiest and most obvious target for a defamation action will be these people or entities. Those hosting discussion boards or facilitating bloggers are particularly at risk.

Publication on the net is somewhat different to other forms of publication in that a person must first upload the material in an electronic form to the ISP.[5] In effect, the ISP then 'publishes' the material to the net. An ISP has little control over content for general email traffic, but does have control over its bulletin boards, and possibly over its customers' individual websites, blogs and so on. The difference in use has become important in determining jurisdictional

issues but may also be important in determining the liability of an ISP or ICH as a primary publisher.

Given the global nature of the internet, it is useful to compare the attempts of different jurisdictions to deal with this very real problem.

US position

Prior to 1996, a plaintiff had to show that the ISP had knowledge of the contents of allegedly defamatory statements on the system before it could be held liable. In *Cubby Inc v CompuServe Inc*,[6] the plaintiff could not show this and the ISP was therefore not liable for defamatory statements and succeeded in a defence of innocent dissemination. On the other hand, in *Stratton Oakmont v Prodigy Services Co*,[7] the ISP exercised a certain amount of editorial control over its bulletin boards by deleting messages that fell outside its published guidelines. In these circumstances, the ISP was held to be a publisher for defamation purposes. In a later case involving the same ISP, *Lunney v Prodigy Services Co*,[8] the ISP had ceased to exercise editorial control over its bulletin boards and it was found by the Court that the ISP had not published the material.

After 1996, the position in the US was governed by the *Communications Decency Act* 1996. Section 230(c)(1) of that Act provides:

> *'no provider or user of an interactive commuter service shall be treated as the publisher or speaker of any information provided by another information content provider.'*

In effect, the law created an immunity for ISP's who no longer have to concern themselves with defamatory content. In *Zeran v America Online Inc*,[9] an anonymous net user posted a message of the flame variety on an AOL bulletin board advertising t-shirts with slogans glorifying the bombing of the Federal Government building in Oklahoma City. Any person wishing to buy the shirts was instructed to call 'Ken' and was provided with Zeran's home phone number. Zeran received numerous angry and threatening phone calls in response to the posting. Rather than be confronted by the issue of whether the ISP is a publisher for defamation purposes, Zeran sued AOL for negligence in distributing defamatory material which it knew or should have known was defamatory. However, the *Communications Decency Act* 1996 conferred protection on AOL for this publication, which also covered the action for negligence.

English position

In England, section 1 of the *Defamation Act* 1996 (the **Defamation Act**) created a statutory defence of innocent dissemination. Where a publisher establishes that it was not the author, editor or publisher, that it took reasonable care in relation to the publications and that it neither knew or had reason to believe that its actions contributed to the publication, it is not liable for the publication. For the purposes of the Defamation Act, 'publisher' includes operators or providers of access to communication systems by which a defamatory statement is transmitted or made available.

This statutory defence was invoked for the first time before a jury in *MORI v BBC*.[10] Consideration was given to the fact that the BBC exercised reasonable care and had no control over the person making the defamatory statement during a live interview. The judge ruled that in order to gain the protection of the defence, the broadcaster had to show that it had no effective control over the maker of the statement. This case actually settled while the jury was considering its verdict.

In *Godfrey v Demon Internet Limited*,[11] the High Court found that an ISP was the 'publisher' of a defamatory statement anonymously posted on one of its Usenet newsgroups. The case was brought by an English university professor who was allegedly defamed in an newsgroup by an unknown person in the USA. The newsgroup was carried by Demon, one of the UK's largest ISPs. When Godfrey became aware of the defamatory posting, he requested Demon to delete it from its server. Demon refused, even though it had the ability to do so. Godfrey claimed damages in relation to the period after which Demon had been put on notice of the posting and the request for removal had been made. The Court held that ISPs that knowingly carry defamatory material and fail to remove it on request are liable as publishers. Demon could not avail itself of the innocent publication defence provided by the *Defamation Act* as it was put on notice of the posting.

Demon appealed this decision and argued that Godfrey himself deliberately posted the inflammatory statements with a view to launching a vexatious defamation action against it. Demon claimed that this constituted flaming and provoked others to trade insults which Godfrey then claimed were defamatory. The action was settled for an undisclosed sum.

Since August 2002, section 1 of the Defamation Act must be read subject to the Electronic Commerce (EU Directive) Regulations 2002. These Regulations are complex as they distinguish between an ISP acting as a mere conduit, and other more involved actions of an ISP such as caching and hosting. The Regulations grant immunity to ISPs who do not have actual knowledge of *facts or circumstances from which illegal activity or information is apparent'*. Arguably, this does little more than section 1 in any event.

The English Law Commission conducted a preliminary investigation into defamation and the Internet and released a report on the issue in December 2002. The report recommended a review of the way defamation law impacts on ISPs as they face constant pressure to remove material from their sites without real consideration of the issues, simply because they are under threat of losing their section 1 defence. This conflicts with the emphasis placed on freedom of expression under the European Convention of Human Rights. There is also concern that businesses and corporations are increasingly using legal threats against ISPs to close down protest websites set up by customer groups. Ideas discussed by the Law Commission included an immunity for ISPs similar to that in the USA, or an extension of the innocent dissemination defence to

cover, for example, dealings with complaints under an industry code.[12]

Australia

Obviously, an ISP cannot effectively monitor all information published across its service and, arguably, should not be responsible for the defamatory publications of its users. However, the law in Australia makes those who are within the umbrella of 'publisher' liable.

In Australia, the common law defence of innocent dissemination is available but is very narrow in its operation. This was illustrated in *Thompson v Australian Capital Television*.[13] In that case, Channel 7 claimed that by relaying a live TV show to the ACT from Channel 9 in New South Wales, it simply acted as a subordinate publisher and disseminated the work of the actual publisher without knowledge or control of the content of the program, akin to a printer or newspaper seller.

The High Court saw no logical reason why the defence of innocent dissemination should not be available to television broadcasts as well as printed material, but in this situation Channel 7 had the ability to control and supervise the material it televised. Even though the program was a live program, it was Channel 7's decision that the transmission of the program should be near instantaneous and it was well aware of the fact that it was a live-to-air current affairs programme which carried a high risk of defamation. Channel 7 was not therefore a subordinate publisher in this instance.

The question of innocent dissemination will be a question of fact in each case and any party seeking to rely upon this defence will realistically need to establish that it had no knowledge of even the possibility of any defamatory content. Needless to say, this is unlikely to be the case for an ISP or ICH hosting a discussion board or weblog.

The *Broadcasting Services Amendment (Online Services) Act* 1999 (the **Act**) amended the *Broadcasting Services Act* 1992 and provided a statutory framework for the regulation of content of online services.

The Act contains a provision which although not intended,[14] provides a statutory innocent dissemination defence for ISPs and ICHs. The two are distinguished in the Act in that ISPs offer access to the Internet whereas an ICH may only host Internet content without providing any net connection. 'Internet content' excludes email, but would seem to include those who create their own websites.

Section 91(1) of the Act provides 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:

1. subjects, or would have the effect (whether direct or indirect) of subjecting, an ICH or an ISP to liability (whether criminal or civil) in respect of hosting/carrying particular Internet content in a case where the ICH/ISP was not aware of the nature of the Internet content; or
2. requires, or would have the effect (whether direct or indirect) of requiring, an ICH or ISP to monitor, make enquiries about, or keep records of Internet content hosted/carried by the ICH/ISP.

The onus of proving non-awareness falls on the ISP/ICH. Every ISP/ICH must therefore see or hear no evil. An ISP will only be rewarded if it goes out its way to ignore the contents of its system and keep its head buried in the sand! There is no requirement for reasonable care, as there is with the English statutory defence. The only condition for the removal of the defence is when the ISP/ICH is put on notice of defamatory material and then fails to remove it.

The section uses the words *'not aware of the nature of the Internet content'*. What does 'nature' mean? Does it mean defamatory? Is an ISP/ICH expected to know what amounts to defamatory words? There may be something grossly defamatory to someone, but which on its face appears innocuous to those without knowledge of certain facts. There may be something which is defamatory but defensible, under fair comment for example. Despite this, if the ISP/ICH knows it is there or is told that it is defamatory by anyone then, regardless of these issues, it must remove the material or lose the defence.

There is a further provision in the Act[15] which protects ISPs and ICHs from civil liability including defamation where they have acted in compliance with an industry code registered under the Act. An Internet Industry Code of Practice, prepared by Internet Industry Association, has now been registered under the Act (among others).

Proposed changes in Australia

The Federal Attorney General, recently proposed the introduction of uniform defamation laws across Australia. Although the issue is at the consultation stage, the Attorney General has indicated that these changes will be pushed hard if the government is re-elected in October.

Submissions made in response to the proposal by media interest groups have highlighted the shortcomings of the existing law of defamation in so far as it applies to the liability of ISPs and ICHs.[16] They submit that the law should grant ISPs and ICHs a clear immunity from liability under defamation law, subject to a notification regime in which liability arises only where a notification is received as to potentially defamatory material and is ignored. It has also been suggested that an international approach to defamation law should be considered, particularly from the point of view of bringing Australian law into line with the US approach.

In his revised outline of a possible national defamation law,[17] the Attorney General simply proposed a regime for ISP's and ICH's which 'would continue to give effect to the current policy of the Broadcasting Services Act.'[18] This would simply double up on the existing Commonwealth law. It is difficult to see why this should be included if the only reason is to have it as part of a uniform code.

It seems no real attention has been paid to problems pointed out with the Broadcasting Services Act defence[19] and to simply cut and paste this into a code would present more problems than it would solve.

In conclusion it is worth noting that the unique qualities of the net along with the informality of net culture may extend to a reluctance on the part of net participants to pursue defamation proceedings. Despite the potentially enormous scope for actions against ISPs and ICHs, in reality there has been surprisingly little litigation as a result. Although today's blogs and flames will never become tomorrow's fish and chip wrapping, there is perhaps a culture evolving of user acceptance giving rise to a level of tolerance previously unseen in other forms of media.

* The author would also like to acknowledge the assistance of Dougal Langusch in writing this article.

1 Sydney Morning Herald 28 August 2004 article entitled 'Pest Control' by Edmund Tadres.

2 'Netiquette', www.albion.com/netiquette/book

3 http://en.wikipedia.org/wiki/Internet_troll #Trolling_in_the_1990s which in turn attributes this quote to Donath, 1999

4 www.elearnspace.org/Articles/blogging part_1.htm

5 In fact a plaintiff must establish that a defendant uploaded material onto the net to prove publication – Ezzo v Grille [2004] NSWSC 522

6 (1991) 776 F Supp 135

7 (1995) 23 Media L Rep 1794 NY

8 New York Court of Appeal, 2 December 1999, unreported.

9 [1997] 129 F3d 327

10 (1999) unreported

11 [1999] 4 All ER 342

12 Law Commission – Defamation and the Internet Scoping Study No. 2, December 2002

13 (1996) 71 ALJR 131

14 Curiously, the Explanatory Memorandum states that the purpose of this section is to ensure that the Commonwealth maintains control over regulating the activities of ISPs and ICHs. Presumably to prevent states and territories regulating such entities on offensive content, but it is certainly broad enough to include defamation also.

15 section 88.

16 Combined Media Defamation Reform Group, Submission in Response to Outline of Possible National Defamation Law – Attorney General's Discussion Paper, March 2004

17 Attorney General's Department July 2004

18 above at p25

19 For example the Act excludes email, certain video and radio streaming, voice telephony and of course discourages ISP's and ICH's from monitoring content by the nature of the defence. For a more detailed analysis of the Act see Eisenberg J, 'Safely out of site: the impact of the new online content legislation on defamation law' (2000) 23 UNSW Law Journal; Collins M,'Liability of internet intermediaries in Australian defamation law' (2000) Media& Arts Law Review 209.

auDA Panel reviews domain name policy rules

Alice Grey, Paralegal, Freehills

On 9 August 2004, .au Domain Administration's (**auDA**) Name Policy Review Panel (**Panel**) released[1] an Issues Paper[2] as part of its review of domain name eligibility and allocation policy rules for open second level domains. The Panel was created in July 2004 to examine the domain name policy rules and provide recommendations to the auDA Board about any necessary changes to the policy.

The issues which the Panel has identified for consideration include:

- the integrity of the Australian Domain Name System (**DNS**) and verification of registrant identity
- opening of the Australian DNS to non-Australian registrants, and
- the length of domain name licence periods.

The Panel sought feedback on the matters discussed in the Issues Paper. Comments were due by 30 August 2004.

1 "auDA Panel reviews domain name policy rules", auDA media release, 9 August 2004. See: http://www.auda.com.au/news.php?newsid=17 (last accessed 28 September 2004).

2 *Domain Name Eligibility and Allocation Policy Rules for the Open 2LDs Issues Paper - August 2004*, auDA Name Policy Review Panel. See: http://www.auda.com.au/pdf/nprp-public1.pdf (last accessed 28 September 2004).