

MICHELLE NENA GOODING

**“DEFAMATION AND THE INTERNET : A TANGLED WEB
OF LEGAL ISSUES IN A BORDERLESS ENVIRONMENT”**

Submitted for the LLB (Honours) Degree at
Victoria University of Wellington

1 SEPTEMBER 1997

G652

GOODING, M.N.

Defamation and the internet.

e
AS741
VUW
A66
G652
1997



TABLE OF CONTENTS

V	REFORM PROPOSALS	26
I	INTRODUCTION	1
II	THE INTERNET	3
A	<i>What is Cyberspace and the Internet?</i>	3
III	DEFAMATION LAW IN NEW ZEALAND	6
A	<i>Ingredients of the Tort of Defamation</i>	8
1	<i>Defamatory statement</i>	8
2	<i>Identifying the plaintiff</i>	9
3	<i>Publication by defendant</i>	9
B	<i>Innocent Dissemination</i>	11
C	<i>Remedies</i>	12
D	<i>Defences</i>	12
1	<i>Truth</i>	13
2	<i>Honest opinion</i>	13
(a)	The opinion must be genuine	13
(b)	The opinion must be based on true facts	13
IV	POLICY ARGUMENTS FOR AND AGAINST LIABILITY FOR DEFAMATORY STATEMENTS ON THE INTERNET	15
A	<i>Originating Author</i>	15
B	<i>The Position of ISPs</i>	16
1	<i>ISPs as actual publishers</i>	17
2	<i>ISPs as mere distributors</i>	17
(a)	<i>Cubby, Inc. v CompuServe Inc.</i>	18
(b)	<i>Stratton Oakmont v Prodigy Services Co.</i>	19
(c)	<i>Thompson v Australian Capital Television</i>	20
C	<i>Conflict of Laws, Jurisdiction and Forum Shopping</i>	23

V	REFORM PROPOSALS	26
	A <i>Reform Options</i>	26
	1 <i>Self-regulation</i>	26
	2 <i>A new tort of defamation</i>	28
	3 <i>Defamation legislation encompassing the Internet</i>	29
	B <i>Protecting ISPs</i>	29
	1 <i>A code of conduct</i>	30
	2 <i>Avoiding a finding of liability for an ISP</i>	30
VI	CONCLUSION	32

BIBLIOGRAPHY

APPENDIX I

Assuming none of the above is true, as an aggrieved retailer you are faced with several concerns: what can be done to remedy this situation in the first instance; and, secondly, who should be held responsible for the injury and damage to your reputation that this might will inevitably cause?

The rapid expansion and novelty of the Internet has led, amongst other things, to a tangled web of legal issues. Some of these difficulties are unique to cyberspace and arise out of the very elements that characterise the Internet, particularly the ability to communicate information around the globe in a fraction of time for minimal outlay. The nature and scope of the Internet and its related services presents opportunities for mischief: anyone can insert defamatory material about another or in the name of an innocent third party. For example, the wording of advertisements can be changed or messages can be trapped, amended and then later sent on. This global information explosion, coupled with the increasing use of personal computers has meant that the laws of all countries of the world are struggling to keep up with the rapid development and uses of the Internet.

I INTRODUCTION

Imagine showing a group of friends the joys of the Internet as you prepare to surf your favourite bulletin board or discussion group - "Rhubarb". Suddenly, for all the world to see (including the gathering of friends behind you) is the following:

"(Your name) of 123 Computer Co. is a dishonest, thieving, lying computer retailer. The hardware is either "hot" or used, is sold as new and the software is largely pirated from overseas. In addition to this, s/he has five children out of wedlock and kicks cats for fun.

Signed - A Concerned (Ex) Customer."

Assuming none of the above is true, as an aggrieved retailer you are faced with several concerns: what can be done to remedy this slur in the first instance; and secondly, who should be held responsible for the injury and damage to your reputation that this slight will inevitably cause?

The rapid expansion and novelty of the Internet has led, amongst other things, to a tangled web of legal issues. Some of these difficulties are unique to cyberspace and arise out of the very elements that characterise the Internet, particularly the ability to communicate information around the globe in a fraction of time for minimal outlay. The nature and scope of the Internet and its related services presents opportunities for mischief; anyone can insert defamatory material about another or in the name of an innocent third party. For example, the wording of advertisements can be changed or messages can be trapped, amended and then later sent on. This global information explosion, coupled with the increasing use of personal computers has meant that the laws of all countries of the world are struggling to keep up with the rapid development and uses of the Internet.

This paper examines a traditional legal concept and attempts to apply it to a dynamic revolutionary new method of communication. The discussion advanced throughout this paper particularly focuses on difficulties arising from instances of defamation on the Internet that originate from bulletin boards, newsgroups and e-mail. In examining this topic, Part II of this paper explains the origins and capabilities of cyberspace and the Internet. A consideration of the traditional approach to defamation law in New Zealand follows in Part III, specifically identifying the purpose, relevant elements and limitations of this particular branch of the law. Part IV canvasses policy arguments for and against liability of defamatory statements published on the Internet; the practicalities of determining who may be liable is considered and relevant case law from the United States and Australia is assessed. In evaluating ideas for reform, I have concluded this paper by advancing some suggestions which, although not resolving all the difficulties highlighted (in this paper), may assist both users and Internet Service Providers in avoiding a finding of liability for defamation.

Academic writing in this area is largely focused on critiques of the case law to date, particularly the inadequacies pertaining to the *CompuServe* and *Prodigy* decisions originating from the United States. In terms of originality, this paper attempts to develop the debate a step further by evaluating and developing existing policy arguments to suggest ideas for reforming the complex area of defamation and the Internet. In addition, precautions service providers might consider adopting are suggested as a means of avoiding liability for defamation.

¹ William Gibson *Neuromancer* (HarperCollins, London, 1984).

² Peter Wiggin *Wild Kevic: Every New Zealander's Guide to the Internet* (Orion Bay Press, Christchurch, 1996).

II THE INTERNET

In the last two decades the increased availability of computers has revolutionised fundamental methods of communication. Through the use of computers and the Internet, more people have direct access to increasing amounts of information.

A *What is Cyberspace and the Internet?*

Cyberspace as a concept and a "place" is the product of the mind of William Gibson, an author who began writing novels and short stories in the early 1980s. His 1984 book *Neuromancer*¹ spoke of the intensity with which people played at and with video games and computers; developing a belief of some kind of actual kind of *space* behind the screen - some *place* that you cannot see, but you know is there. It was this space or place that Gibson called "cyberspace", the locale of his novels, a computer-imaged and generated landscape which his characters could enter by plugging in.

As it exists today, the Internet represents the "real" operation of Gibson's ideas as a medium of communication which operates at the speed of light and provides access to all of the data in all of the computers of humankind. It affords people the opportunity to exercise one of our most highly developed capacities, the ability to communicate freely with each other, through the Internet.

The Internet can be described as the ultimate global network. It is an **interaction** or **interconnection** between computer **networks** where a set of standard agreements (protocols) among thousands of computer networks defines and makes the Internet unique.² These agreements define how the network computers will talk to each other and exchange information. The Internet consists of voluntary associations of computer networks which, by their very participation, express their willingness to share knowledge, resources and ideas.

¹ William Gibson *Neuromancer* (HarperCollins, London, 1984).

² Peter Wiggin *Wired Kiwis: Every New Zealander's Guide to the Internet* (Shoal Bay Press, Christchurch, 1996).

To its founders, the Internet constituted a vehicle for communicating information, built on the premise that sharing information and ideas would promote science and education. The Internet began in the early 1970s as a research initiative by the United States military where efforts focused on creating computer networks that could survive enemy attack on one or more locations around the country. If, for example, one link in the chain of communication was removed or destroyed, the information could still reach its intended destination by simply finding another path or way around. The method devised was so robust that it soon became a standard for computer communication between machines around the world.³ Enhancements and upgrades continued throughout the mid-1980s when scientific and educational institutions began to realise the tremendous possibilities for communications. Today, the Internet's viability has been accepted by individuals, small businesses, corporations, governments and universities around the world. New Zealand has not ignored this worldwide trend; as of July 1996 New Zealand had 77,886 host computers on the Internet, representing over 120,000 users.⁴ Firmly enmeshed in the "worldwide web", the New Zealand trend shows no signs of abating; daily more and more New Zealanders add to the growing population of over 40 million users in 125 countries.⁵

The Internet is truly an international structure. It has no base in any one country or region, is not owned by anyone and has no controlling computer or governing body. Its core activities include services such as electronic mail (e-mail), newsgroups (electronic discussion or bulletin boards), file transfer and on-line conversation (conferencing which is typed and immediately displayed to other users of the facility). Electronic interactive services such as on-line information are rapidly becoming one of the most efficient and prevalent forms of communication providing access across geographical boundaries, time, language and race.

³ Above n 2, 8.

⁴ Above n 2, 10.

⁵ Jeffrey M Taylor "Liability of Usenet Moderators for defamation published by others: Flinging the law of defamation into Cyberspace" (1995) 47 Florida Law Review 247.

Communication is via packets of information which are transferred from one place to another and operate similarly to a postal service. Each packet of information is placed inside an "envelope" which contains both the source and destination address. The information is then transported to its destination by communicating with another computer on the network. It is then temporarily stored before communicating with a third computer until ultimately reaching the end-user whose access to the Internet is via an "on-ramp" provided by an Internet service provider. As a post office would sort and deliver mail to each house with a unique address, each computer has a unique Internet address; deliveries are then forwarded to their intended destination, scanned, reassembled and re-imaged on a remote computer screen.

The Internet symbolises what must be the closest thing any person can get to a wealth of infinite knowledge at the touch of a few keystrokes. The Internet's potential is slowly being realised and integrated into mainstream society, for example not only can you view the latest pictures of Mars or tour the Louvre in Paris, but one can also purchase books, order pizzas and even do the grocery shopping over the Internet.

Despite its large size and increasing worldwide usage, the Internet remains largely unregulated. For the Internet to fulfil its potential as a mainstream tool in society, it will require some sort of regulation along with other conventional methods of communication and broadcasting. The legal implications are numerous and often ignored by users, operators and service providers (who supply on-line services as "on-ramps" into the Internet). Because the Internet is a dynamic creature, changing, sometimes significantly, literally each moment, its future is both undefined and unknowable. Uncomplicated access and easy reproduction and transfer of information open up opportunities for circulation of ideas and information but challenge traditional laws that govern communications. The challenge for the legislature, law enforcement, Internet service providers (hereafter referred to as "ISP") and Internet users is to reach a fair balance between the competing interests of free exchange of ideas, frank and open expression and protecting reputations from unwarranted or unjustified attack via the Internet.

III DEFAMATION LAW IN NEW ZEALAND

Stephen O'Gorman describes the evolution of defamation law as:⁶

Historically based on the need to keep the peace, a judicial remedy to stop people taking retribution into their own hands, the law of defamation is now concerned with the protection of reputation from unwarranted attack.

At its most basic level, the essence of this branch of tort law can be summarised as material that is published about an identifiable person which tends to lower that person in the estimation of right-thinking members of society. Assuming all elements of the cause of action are proven, any such material is actionable with a remedy in damages⁷ unless the publisher establishes a defence provided by law. To succeed in an action for defamation, the plaintiff must establish the following:

- (a) a defamatory statement has been made;
- (b) the statement is about the plaintiff; and
- (c) the statement has been published by the defendant.

The enactment, in 1992, of new legislation to amend the law relating to defamation and other malicious falsehoods does not attempt to significantly transform earlier defamation law. Instead, the Defamation Act 1992 (hereafter "the Act") serves to placate previous complexities and ease the rigidity of earlier law.⁸

⁶ Stephen O'Gorman "Defamation and the Internet" Internet Australasia (November 1995, Volume 1, Issue 11, p 28).

⁷ While not the only remedy provided by the Defamation Act 1992, damages are perhaps the most commonly sought form of redress in defamation actions. Typically compensatory in nature, an award of damages purports to restore the plaintiff to the position he or she would have been in had the defamation not occurred. See further discussion in this paper and Part III of the Defamation Act 1992 for additional remedies.

⁸ Stephen Todd (ed) *The Law of Torts in New Zealand* (2 ed, Brooker's Limited, Wellington, 1997) 853.

In particular, the new Act has reformed defamation law in New Zealand in the following two relevant ways:

- (1) Section 4 removes the distinction between libel and slander.⁹ Removal of the requirement to allege or prove special damage in slander proceedings now means the rules are the same for all kinds of defamation.
- (2) Defamation now only exists as a civil cause of action, a tort. Section 56(2) repeals defamation as a criminal offence where publication was deemed likely to disturb the peace or would seriously affect the defamed person's reputation.

As noted above there is no longer a legal distinction in New Zealand between libel and slander.¹⁰ The following Internet services, however, can be classified as parallel to traditional modes of communication and, as such, fall under the defamation umbrella:

- E-mail:¹¹ The ability to make hard copies and circulate widely is uncomplicated and should be regarded as the paper equivalent to conventional letters;
- Home pages: Electronic publishing on the "World Wide Web" may consist of pictures or words. Humour, cartoons and satire can constitute defamation of one's character or traits if they cannot be proven true.¹²
- On-line chat: Real-time conversation or text, is similar to slander on a telephone system and should be treated as such.

⁹ *Halsbury's Laws of England* (4 ed, Butterworths, London, 1979) vol 28, Libel and Slander, para 1, p 3 defines libel as a defamatory statement made in writing or printing or some other permanent form whereby the law presumes damages. Slander, on the other hand, is oral in nature or exists in some other transient form and is generally not actionable at common law without proof of actual or special damage.

¹⁰ See s4 of the Act.

¹¹ Provided distribution to more than one person occurs e.g. "mail-outs".

¹² Above n 8, 858.

- Bulletin boards: News and varied interest discussion groups can perhaps be classified as not dissimilar from broadcasts.

A Ingredients of the Tort of Defamation

As noted above, a plaintiff must establish three elements in order to prove a case of defamation.

1 Defamatory statement

The traditional common law approach to defamation requires the plaintiff be lowered in the estimation of society. A defamatory statement may tend to make others shun and avoid him or her, or may be calculated to injure the plaintiff's reputation so as to subject him or her to ridicule, contempt or hatred.¹³ Essentially, a defamatory statement must be more than simply false; it must also reflect adversely on the reputation of the plaintiff.¹⁴

Intention is not a relevant consideration in determining whether a statement constitutes defamation. A court will consider what the words actually convey to a reasonable person rather than looking to what the defendant intended to impart through the publication. Even without intending to defame someone as such, a person will, therefore, remain liable for material which is defamatory in nature.

Using the example in Part I of this paper to illustrate defamation in the context of the Internet, a statement exists which is clearly defamatory of the plaintiff. The impact of such allegations, which appear on a widely read bulletin board, is likely to not only lower the plaintiff in the eyes of the public, but also cause others to treat him or her with contempt or be shunned and avoided. Not only is the statement false, it is likely to have serious repercussions for the plaintiff's personal and business reputations by

¹³ Above n 8, 854.

¹⁴ Above n 9, para 6, p 5. An action for defamation does not lie in respect of defaming a dead person.

alleging, as a statement of fact, the plaintiff's propensity for immoral acts and lack of business ethics.

2 *Identifying the plaintiff*

The plaintiff must prove the published words are defamatory of him or her, namely that it is the plaintiff who has been defamed. The requisite test is "whether reasonable persons would reasonably believe that the words referred to the plaintiff".¹⁵ As a result, even accidental references to the plaintiff, for example someone with the same name or whose circumstances fit the situation, will fall into this category. In addition, a company can bring an action in defamation where statements affect its business or trading reputation.¹⁶

Again using the above example to demonstrate the Internet context, it is a relatively simple task to construe the note appearing on the bulletin board as referring to the plaintiff. As the requirement for a defamatory statement has been met above, this limb identifying the plaintiff constitutes the second element of a successful defamation action. In addition, a person of the same name operating a computer company of the same name, even on the other side of the world, will also have grounds for a defamation action against the defendant even though the material is not meant to refer specifically to them. The fact that a defamatory statement exists and a reasonable person could believe it to refer to a second person on the other side of the world leaves the defendant open to further liability.

3 *Publication by defendant*

The third ingredient the plaintiff is required to establish is that the statement is published to a third person, namely to someone other than the plaintiff. Whether the facts constitute publication is a question of law to be decided by the Judge. Publication

¹⁵ Above n 8, 871.

¹⁶ For a recent New Zealand example where a company's trading reputation was at stake, see *Mount Cook Group Ltd v Johnstone Motors Ltd* [1990] 2 NZLR 488.

can be made through the media to a wide audience or can be in the form of disclosure to one other person or a small group.¹⁷ In addition, repetition of a statement constitutes a new publication and consequently a new cause of action exists against the party repeating or republishing the statement.

It is this third ingredient of defamation that poses many of the obstacles likely to arise in an Internet context. First, an issue exists in terms of publication and whether material that can be accessed via the Internet constitutes publication as such. A matter for particular concern is whether, in merely being a vehicle for providing access to the Internet, an ISP can be deemed to have "published" the information at issue. In this respect, I would suggest that it is neither practical nor equitable to place responsibility for all Internet content with ISPs. I would submit that rather, they should be responsible for material originating at their site. Similarly with e-mail transmissions, an ISP merely provides the facility and should not therefore be liable for any defamatory material that is transmitted. The missing ingredient is the ability to exercise control.

A second difficulty lies in identifying the author or publisher: the nature and scope of the Internet means opportunities for tracing the original author may be limited and presents practical difficulties in a technical sense. Laying blame at the feet of a service provider, even if the organisation had no viable means of knowing about the defamatory matter, therefore, may prove to be the only recourse available that an aggrieved person has in terms of vindicating the wrong. Finally, as the Internet knows no bounds and exists in a borderless environment, a significant problem is presented when consideration is given to the fact that publication can occur simultaneously in different legal jurisdictions. The difficulty from this point of view is determining which, if any, law is applicable to the situation. Specific issues arising from identity, knowledge and jurisdiction are discussed in greater detail in Part IV of this paper.

¹⁷

Above n 8, 878.

B Innocent Dissemination

Particularly relevant to the scope of this paper is section 21 which provides a defence to persons who have published matter in the capacity of, or as employee or agent of, a processor or distributor.¹⁸ Persons involved in "innocent dissemination" can avail themselves of this defence by proving:¹⁹

- "(a) That that person did not know that the matter contained the material that is alleged to be defamatory; and*
- (b) That that person did not know that the matter was of a character likely to contain material of a defamatory nature; and*
- (c) That that person's lack of knowledge was not due to any negligence on that person's part."*

When considering an action concerning defamation and the Internet, an issue arises as against whom a probable cause of action might lie. Defamation law attributes maximum liability to the originating author of published defamatory statements. Secondary publishers, such as booksellers and newsagents, however, are not liable if the publication is deemed to be innocent.²⁰ This means that liability would accrue if a publisher in this sense knew or should have known the material contained defamatory matter.

Pertinent to the example at the beginning of this paper, assuming the "Concerned (Ex) Customer" is unable to be traced or identified, the plaintiff, in seeking to vindicate their reputation, may seek to bring proceedings against those who handle information that appears on the Internet (for example, bulletin board or discussion group monitors, their employers or the providers of the particular service). If this occurs, service providers will argue they come within the scope of the defence provided by section 21. This presents the problem that, despite its recent enactment amending previous anomalies in

¹⁸ Section 2(1) defines "distributor" as including a bookseller or librarian and "processor" as a person who prints or reproduces, or plays a role in printing or reproducing, any matter.

¹⁹ See s21.

²⁰ Above n 19.

the law, the Defamation Act 1992 is not worded with the Internet in mind. The issue whether ISPs are covered by the defence in section 21 has yet to be determined in the New Zealand courts. However, it is likely that a New Zealand court would follow the lead of United States and Australian determinations in making the defence of innocent dissemination available in an Internet context. The inappropriateness of marrying current defamation law with such a dynamic creature as the Internet is discussed more fully later in this paper.

C Remedies

Remedies for defamation are set out in Part III of the Act. In an action for defamation, damages constitute the most common form of redress and are awarded to compensate the plaintiff for:

- (1) the injury to his or her reputation; and
- (2) the hurt to his or her feelings.

The underlying purpose of compensating the victim is to vindicate the plaintiff to the public and attempt to restore him or her to the position he or she was in, had the defamation not occurred.

D Defences

Part II of the Act provides a number of recognised defences to an action of defamation, namely truth, honest opinion, and absolute and qualified privilege. The two most pertinent defences relating to subject matter considered in this paper are set out below.

1 *Truth*

Previously known as the defence of justification, this defence will only succeed if the defendant can satisfy the court that the imputations were either true or the substance is not materially different from the truth.²¹ The rationale behind this defence lies in the notion that a person is entitled only to a reputation worthy of their behaviour. Therefore, if the computer retailer in the example already mentioned was found to be dealing in pirated or second hand goods and selling them as new and legitimate licensed software, the alleged wrongdoer would have a defence to the charge of defamation as the accusations are truthful. Similarly, if the plaintiff only has four children out of wedlock or kicks guinea pigs for amusement, because the substance of the imputations is not materially different from the truth, the defence will still apply.

2 *Honest opinion*

Prior to the commencement of the 1992 Act, this defence was known as the defence of fair comment. The defence of honest opinion embodies the very essence of free speech: the idea that citizens should be able to express their views freely without fear of retribution or censorship. Sections 9 to 12 of the Act specify a number of conditions which must first be complied with before the defence of honest opinion will succeed.

(a) The opinion must be genuine

Section 10 requires the opinion expressed to be the genuine opinion, and recognisable as such, of the defendant. Further, the existence of malice in motivating publication will not preclude a defence of honest opinion.

(b) The opinion must be based on true facts

Section 11 provides the defendant prove only those statements of fact which are relevant and form the basis of the opinion. Proof of the truth of any statement of fact not related to the opinion is not required.

²¹ Sections 8(3)(a) and 8(3)(b).

While the overall effect of the new legislation cannot be said to have completely reformed the law of defamation in New Zealand, it has attempted to simplify some of the more complex areas of the law. Protecting one's reputation from unjustified malignment is both important and necessary in today's society. However, finding the balance between protecting one's reputation and freedom of expression (which has come to be accepted as an integral feature of the Internet) is not without complications. Tipping the balance too far toward protecting reputations is arguably a breach of s14 of the New Zealand Bill of Rights Act 1990; freedom of expression is defined in that section as "including the freedom to seek, receive, and impart information and opinions of any kind in any form." This provision would therefore cover any information on the Internet and other on-line systems. These and other difficulties are compounded when existing legislation is mapped onto new, dynamic technologies and methods of communication, such as that characterised by the Internet, which the legislation does not specifically take into account.

In terms of the scope of this paper, a primary publisher will be in a better position to point to the truth behind an alleged defamatory statement. As the first author, a primary publisher may also be able to identify information which clarifies the statement as being his or her honest opinion. The situation becomes more complex when considering the position of secondary publishers such as ISPs. In the first instance, it would be difficult for an ISP to absolve itself from liability by proving the truth of the imputation. An ISP is unlikely to possess any knowledge about the background of the parties involved and would be hard pressed to verify each piece of information that passed through its services due to the sheer volume and speed with which information can be uploaded. Similarly, a further problem exists with the defence of honest opinion in that the statement is not that of the ISP but rather belongs to the original author. It is unlikely that an ISP, as a secondary publisher, would be able to engage this defence because the statement is clearly not the genuine or honest opinion of the ISP. As a result, it is unreasonable and impractical to expect a service provider to defend a charge of defamation using either of these existing defences.

IV POLICY ARGUMENTS FOR AND AGAINST LIABILITY FOR DEFAMATORY STATEMENTS ON THE INTERNET

The Internet poses profound challenges to fundamental requirements for any effective law. Where publication of defamatory statements over the Internet occurs, three core issues arise when considering the likelihood of a successful legal action; namely, identifying the wrongdoer, the level of knowledge that is required to satisfy a finding of liability in a defamation action; and complications that exist due to different legal jurisdictions.

A *Originating Author*

It is clear law that a prima facie case of strict liability rests with the originating author or publisher for initial defamatory publications. The structure of the Internet, however, means that often an original author will be anonymous or hiding behind a pseudonym so that the origin of the defamatory message may be untraceable. For any law to be enforceable there must be an identifiable person to whom liability is attributed. On the Internet, however, one's virtual personality can be hidden, altered and falsified with no simple method of linking a person's on-line identity and the real person. In cases where it is possible to identify an original author, however, case law suggests that liability may be fixed relatively easily against the alleged wrongdoer.

The Australian case of *Rindos v Hardwick*²² is one of the first reported cases involving defamation and electronic newsgroups and confirms the application of defamation law to material published in cyberspace. The plaintiff (Rindos), an internationally renowned anthropologist, was denied tenure and dismissed from the University of Western Australia for insufficient productivity. In response to this, an American criticised the University of Western Australia's actions via an anthropology bulletin

²²

(Unreported judgment 940164, 31/3/94, Supreme Court of Western Australia, Ipp J).

board.²³ The defendant, Hardwick, replying in his own name, posted his personal views on the matter alleging that Rindos had engaged in sexual misconduct with a local boy "Puppy" and further, that the anthropologist had no genuine academic ability and relied on bullying and berating others rather than immersing himself in appropriate research. The Supreme Court of Western Australia found in favour of the plaintiff, granting him \$40,000 in compensation to vindicate his reputation to the public.²⁴ Justice Ipp found Hardwick's posting to have seriously defamed the plaintiff; the inference being that the matters had a bearing on his failure to be awarded tenure. Because the imputations were published in academic circles and Rindos had a high international standing, the defamatory remarks were likely to have harmful effects, causing damage to both Rindos' personal and professional reputation.

The effect of the *Rindos* decision is significant in several ways. First, the decision confirms the application of defamation law to new methods of communication such as the Internet. Secondly, any doubt that a news item on an electronic bulletin board constitutes publication is removed and; thirdly, that an author, once identified, will be held liable for publishing defamatory material on the Internet.

B The Position of ISPs

The issues become more complex when we consider liability that is removed from the original author of defamatory material. As discussed above, it may be problematic to prove a particular individual, as opposed to a particular computer, actually sent the offending message. For example, assuming the computer with the originating message can be identified, it may be difficult to isolate the offending person in the absence of a signature or system requiring the use of individual (as opposed to company) passwords. The complexity of the situation is further compounded when computers with access to Internet and e-mail facilities are freely available for employee use which makes it even

²³ Evidence revealed that approximately 23,000 people worldwide had access to the particular bulletin board; messages could remain in the system for days and even weeks depending on computer capacity and volume of messages; and further, items of interest could be printed on hard copy and redistributed.

²⁴ In this case the defendant did not enter an appearance. Judgment by default was consequently granted to the plaintiff.

more difficult to trace the author. Situations such as the one just described with no safeguards in place, leave employers vulnerable as the owner of the computer in defamation proceedings. In addition, an author probably cannot pay more than a modest award should they find themselves embroiled in defamation litigation. Given the perception of deeper pockets and likelihood of insurance cover, ISPs, owners and operators of computers may therefore find themselves exposed as unwilling participants in the litigation.

1 *ISPs as actual publishers*

An issue arises as to whether an ISP, in providing an access ramp onto the Internet, should be characterised as a primary publisher (for example, as a newspaper or broadcaster) of defamatory statements accruing maximum liability as if the ISP were the actual speaker and akin to a real world publisher. As a matter of policy and in terms of practicality, it will be necessary for the courts to establish to what extent, and indeed whether, an ISP has the ability to edit or screen Internet material that it purports to exercise control over. The question to be decided is whether an ISP can be characterised as part of the publication process and therefore liable as a party to the publication. Each service provider's involvement with information, however, will vary. Liability will depend on the extent of involvement and the control that each service provider exercises. I would contend that where information from a third party is made available via the Internet by an ISP and there is no direct control over the information that materialises, the ISP ought to then be categorised as a distributor within the principle of innocent dissemination in section 21 of the Act.

2 *ISPs as mere distributors*

A further issue in the primary and secondary publisher debate is whether liability should merely extend to a distributor standard, for example, as a bookseller or newsagent. Classification as a secondary publisher or distributor (under the defence of innocent dissemination) offers greater legal protection to an ISP, conferring liability

only for statements the ISP knew, or ought to have known, were defamatory. As will be discussed later in this paper, knowledge in this respect may be difficult to prove.

A distributor type framework is concerned with principles protecting the free exchange of ideas and information. Placing restrictions on booksellers, for example, confers an onus on them to be aware of the contents of all books in their possession. As a result, placing restrictions on a bookseller subsequently impedes public access to printed matter.²⁵ A publisher framework on the other hand requires communication to a third party to constitute "publication". Each party with a role in the publication process, therefore, can be held liable for publication. This analysis treats the publishing party as analogous to a newspaper; as there is an ability to edit or screen for potentially defamatory matter, the newspaper or broadcaster will be answerable for any publications deemed to be defamatory.²⁶

While limited in number and still in a stage of infancy in relation to development of the law, cases emerging from the United States and Australia appear to have determined contradictory extremes in terms of the publisher and distributor debate. The first two cases originate from the United States where: first, an on-line service provider is held as the functional equivalent of a mere "distributor" of news; and conversely there is authority in a second case for the proposition that the standard of liability to be imposed is that of publisher. A third case illustrates an Australian High Court decision where the defence of innocent dissemination failed.

(a) *Cubby, Inc. v CompuServe Inc.*²⁷

CompuServe developed and provided an on-line general information service that subscribers could access from a personal computer. In exchange for a membership fee and on-line time usage fees, subscribers had access to over 150 special interest forums such as topical databases, interactive conferencing and electronic bulletin boards. At issue were the contents of a journalism forum "Rumourville", the content of which

²⁵ Matthew C Siderits "Defamation in Cyberspace: Reconciling *Cubby, Inc v CompuServe, Inc* and *Stratton Oakmont v Prodigy Services Co*" (1996) 79 Marquette Law Review 1065, 1071.

²⁶ Above n 25, 1072.

²⁷ (1991) 776 F Supp 135.

CompuServe contracted with a separate company to edit, review and control. This arrangement meant that CompuServe had no opportunity to review the contents of Rumourville before it was uploaded and immediately available on-line. A rival database claimed that Rumourville had published false and defamatory statements about it and that CompuServe carried these as part of its journalism forum. CompuServe contended their position as a distributor rather than publisher, denying liability as they neither knew, nor had reason to know, of the defamatory statements.

In this motion for summary judgment, Leisure J found CompuServe's product to be an electronic for-profit library with no more editorial control than a traditional news vendor, library or book store. Furthermore, a lower standard of liability would impose an undue burden on the free flow of information as it would not be feasible for CompuServe to examine all publications. The appropriate standard of liability, therefore, was held to be that of distributor. Having no knowledge nor any reason to know of the alleged defamatory statements, especially given the large number of publications and the speed with which Rumourville was uploaded and available to its subscribers, Leisure J found CompuServe not liable in the absence of any fault.

(b) *Stratton Oakmont v Prodigy Services Co*²⁸

This case involved statements about the plaintiff company made by an unidentified "poster" on Prodigy's "Money Talk"; the leading and most widely read computer bulletin board in the United States, comprising some 60,000 messages daily. In its promotions, Prodigy declared itself a family oriented computer network, holding itself out as an on-line service which exercised stringent editorial control over content. In expressly differentiating itself from competitors, Prodigy was held at the same time to have expressly likened itself to a newspaper. Content guidelines stated any postings in bad taste would be removed when brought to Prodigy's attention; software screening programmes were used to filter out offensive language; duties of Board Leaders included enforcing Prodigy's guidelines and an emergency delete button enabled Board Leaders to remove notes.

²⁸ (1995) 23 Media L Rep 1794.

On the above factual analysis, the Supreme Court held that in using manpower and technology, Prodigy was clearly making decisions as to content and that these decisions constituted editorial control and judgement, necessitating a finding of increased liability. In effect, Prodigy had created an editorial staff of Board Leaders who had continual monitoring ability; as agents, Prodigy was vicariously liable for their actions. The outcome of exercising editorial control confers publisher status on Prodigy with the same responsibilities as a newspaper.

(c) *Thompson v Australian Capital Television*²⁹

In this decision of the Australian High Court, the majority advocates the proposition that "broadcasters" of information are required to exercise due care when broadcasting material that is likely to be controversial and/or defamatory. In this case, the plaintiff sued over a television programme broadcast by the defendant with a licence agreement allowing it to broadcast from a Sydney television station. In mounting a distributor type argument, Australian Capital Television argued its role as that of merely effecting transmission and; further, that nothing in the licence agreement entitled it to vary the material transmitted. The High Court rejected this reasoning to hold that the defendant did not resemble a distributor and; further, that its lack of knowledge of defamatory material was due to its own negligence.³⁰

It is pertinent at this stage to attempt a critique of the American case law. As it stands, the law is uncertain and inconsistent. Academic comment suggests that a combination of the *CompuServe* and *Prodigy* decisions will result in ISPs adopting a hands-off approach to communication via their bulletin board and newsgroup related services which, ultimately, may result in increased defamation on the Internet.³¹ The rationale behind this is that service providers will not take positive action or make attempts to screen out defamatory material for fear they will be subject to a publisher standard of

²⁹ (1994) 54 FCR 513.

³⁰ If the defendant had proven it was not possible to monitor the programme in any practical sense, it is arguable it may more easily have established it was not negligent in failing to regulate the contents.

³¹ See Stephen Dooley "Dealing with defamation on the internet" (1996) 140 Solicitors Journal 46 and R Timothy Muth "Old Doctrines on a New Frontier - Defamation and Jurisdiction in Cyberspace" at <http://www.rbvdnr.com/lit/defame.html>.

accountability. This, however, will depend on personal choices made by ISPs in relation to their decisions to edit bulletin boards and newsgroups. In making the decision to take an overtly hands-off approach to editing Internet material, an ISP may not be liable for defamatory content. Similarly, the decision to exercise editorial control may increase the likelihood of liability being found against an ISP.

It is important to note, however, that both the *CompuServe* and *Prodigy* decisions are dependent on very specific facts. The examples of CompuServe's business being characterised by a contractual agreement with an outside company to review and control the journalism forum and Prodigy holding itself out as a service that exercised rigorous editorial control, are very specific to the individual cases and do not necessarily formulate a blanket precedent for future cases. In response to a complete hands-off stance on the part of service providers, bulletin board hosts or network administrators, however, it may be that a decision of this sort leaves these parties susceptible to negligence claims. The decision to adopt a hands-off approach may, therefore, have ramifications for other aspects of the law depending on whether it would be reasonable to expect an ISP to exercise some forms of control rather than none at all. Assuming this to be the case, then the choice not to exercise control where it would seem reasonable to do so, may be negligent.

Further obstacles encountered in the case law, particularly the *Prodigy* decision, comprise the fact that while newspaper staff have the tools to check the accuracy of the material published, a bulletin board operator does not have the same practical means of doing so. The sheer volume and speed of messages posted to any one bulletin board would render it close to physically impossible to screen every posting for defamatory content. Even if effective screening was able to be carried out, be it random or otherwise, the person monitoring may well not be in a position to determine the truth of any background information that exists which might constitute a defence under Part II of the Act in an action for defamation.

The freedom of expression and exchange of information that users have come to accept and expect on the Internet is also likely to be stifled. Implementation costs are also

likely to be phenomenal: the initial cost of setting up monitoring and control functions which, in conjunction with lost subscribers who object to on-line surveillance, is unlikely to be recovered.

Finally, variations in judicial opinion regarding the defence of innocent dissemination between the United States and Australia highlight further problematic consequences for defamation and the Internet; namely jurisdiction and the issue of forum shopping. While not forming a core part of this paper, these issues are expanded on in a later section.

As discussed above, a degree of legal protection may be afforded to parties who can be classified as innocent disseminators or distributors. For parties falling into this category, liability for defamatory statements will attach only in instances where the party knew or had reason to know of the existence of the defamatory material. Because the foundations of the Internet are so innovative and distinct from traditional entities that defamation law might be applied to, simply mapping the existing legal framework (which does not specifically provide for cyberspace) onto the Internet is problematic. One major obstacle faced by the Internet is the difficulty in attributing knowledge on the part of an ISP.

Cyberspace allows individuals the opportunity of publication to an international audience. Many of these people will not be versed in defamation law, have ready access to lawyers for advice, nor have the resources to compensate someone harmed by the statements they make. Extraordinary amounts of information and data are constantly uploaded into the infinite realms of cyberspace. The majority of computer information services will allow users to upload information onto the service often without vetting or first screening content.³² As a result, ISPs will often have no knowledge of the content and type of material passing through their sites, let alone the means or ability to find out. Yet because of the difficulties associated with locating and

³²

An obvious exception to this relates to information placed by the service provider or operator, for example databases such as LEXIS and WestLaw. See Timothy Arnold-Moore "Legal Pitfalls in Cyberspace: Defamation on Computer Networks" (1994) 5 *Journal of Law and Information Science* 165.

identifying a hidden or anonymous content provider, it will often be a blameless, yet identifiable, service provider from whom redress is sought.

As described at the beginning of this paper, anonymous authors clearly have opportunities for mischief-making on the Internet. Stephen O'Gorman stresses that identification and knowledge may be difficult to prove to the standard required by law. In questioning the application of law in cyberspace, he contends that if liability cannot be attributed then defamation law, as applying to the Internet, is undermined. Further, he argues that if a person's reputation can be so devalued by unpunished attacks then the rationale for penalising an identifiable author becomes less clear.³³

The current regime of defamation law does not adequately represent the realities of service providers and operators on the Internet. Future courts will have to examine the nature and extent of editorial control that is exercised. Given the increasing availability and expansion of the Internet, and the impracticalities that exist relating to the extent of knowledge ISPs are required to possess, it is suggested that it is an onerous burden to place responsibility at the feet of service providers for all material freely available over the Internet.

C Conflict of Laws, Jurisdiction and Forum Shopping

While a full discussion is beyond the scope of this paper, it is important to identify the impact of this further complication as it affects the question of defamation and the Internet. The borderless nature of the Internet means that cyberspace poses critical questions about conflict of laws, jurisdiction, choice of law and forum shopping. In particular, it can be argued that the global nature of the Internet has opened the way to forum shopping. Internationally, the degree to which countries protect their citizens against defamation and the level of damages awarded in defamation actions varies greatly. The result may be that potential plaintiffs in Internet defamation actions will initiate proceedings in jurisdictions with the most restrictive defamation laws.

³³ Above n 6.

In an Internet defamation action, choices of law will be available because the act of defamation occurs in many states or countries simultaneously. The plaintiff may be entitled to sue in any state in which he or she can prove that someone received the defamatory message. Conflict of laws is concerned with cases having a foreign element; that is, contact with a system of law other than that of the particular country. Such contact, in the context of defamation and the Internet, exists because the tort was committed there.³⁴ Conflict of laws is a necessary part of the law of every country. Different countries operate different legal systems containing unique legal rules and adjustment is necessary between them when events are not confined within the borders of a single country.³⁵ This point is particularly relevant to the Internet given its universal scope and disregard for international boundaries.

In terms of jurisdiction, *Halsbury's Laws of England* asserts liability for defamation claims are governed by domestic law if the alleged tort occurred in New Zealand. If the alleged tort was committed overseas, then common law choice of law rules apply. The tort of defamation is further deemed to have been committed in the place *into* which, as opposed to the place *from which*, the defamatory material is communicated.³⁶ In addition, where a New Zealand court and a court of another country have jurisdiction to hear and determine the proceeding, the forum conveniens is the forum in which the proceeding could be more suitably tried in the interests of the parties and in the interests of justice.³⁷

Because single pieces of information are likely to be published simultaneously in multiple countries over the Internet, it is clear from the above that an action may be brought in one country and damages sought with respect to publications in other jurisdictions. The possibility exists, for example, for each publication of defamatory material to be subject to separate actions against publishers around the world. The effect of this means global liability is opened up wherever each publication is received

³⁴ *Halsbury's Laws of England* (4 ed reissue, Butterworths, London, 1996) vol 8(1), Conflict of Laws, para 601, p457.

³⁵ Above n 34, para 602, p457.

³⁶ Above n 34, para 896, p667.

³⁷ *The Laws of New Zealand* Volume 7, Conflict of Laws: Jurisdiction & Foreign Judgments (Butterworths, Wellington, 1996).

around the world. Indeed, in the *Rindos*³⁸ decision, Judge Ipp considered the ramifications of wide publication in assessing the damages payable.

Current legal principles in relation to publication and communication were designed New Zealand's law of jurisdiction derives partly from statute (which has overriding force) and partly from precedent.³⁹ Service can be effected whenever the defendant or his/her agent is in New Zealand. Similarly, if the defendant submits to the jurisdiction of a New Zealand court, a court may be vested with jurisdiction. According to the High Court Rules, service overseas is allowed without the leave of the court.⁴⁰ As far as Internet defamation is concerned, Rule 219(a) allows "statements of claim...to be served out of New Zealand without leave of the Court, where any act or omission for or in respect of which damages are claimed was done or occurred in New Zealand." This subsection appears to be directly applicable to the Internet defamation context. Rule 219(a) would apply in the case of alleged defamation as any publication on the Internet may simultaneously appear on New Zealand computer screens and, therefore, communication of the defamatory material would occur in New Zealand.

Again, while the not the subject of this paper, the issue of forum shopping where a plaintiff can choose a jurisdiction with the fewest defences or narrowest interpretation of them will need to be addressed.⁴¹ Allowing claimants a choice of jurisdiction where the law is likely to be more amenable to their defamation claim is an undesirable manipulation of the law. It is difficult to perceive a means of avoiding this given that different jurisdictions are inevitably involved when considering the Internet. In summary, therefore, electronic communications create difficulties in applying traditional choice of law rules to a tort that may have little relation to a single geographical area. A New Zealand court would be required to develop new methods of dealing with this problem.

³⁸ Above n 22.

³⁹ Laurette Barnard, "New Zealand report on rules for declining to exercise jurisdiction in civil and commercial matters: forum non conveniens, lis pendens" (Wellington, 1994), 1.

⁴⁰ See Rule 219 High Court Rules.

⁴¹ Above n 32, 182.

V REFORM PROPOSALS

Current legal principles in relation to publication and communication were designed pre-cyberspace and have limited ability to embrace the revolutionary fundamentals of the Internet. The law needs clarification in order to remove the turmoil that surrounds defamation without stifling the advantages derived from unencumbered electronic communication. Rather than contorting existing law to encompass the domain of cyberspace, contemporary and innovative solutions (such as the Internet itself) need to be considered.

A Reform Options

There are many and varied options for reforming defamation and the Internet. Because the Internet is a dynamic and evolving creature, there is unlikely to be a solitary effective solution. Academic discussion has considered self-regulation of the Internet;⁴² a new tort of defamation arising out of moderated newsgroups;⁴³ legislative clauses to reform the defence of innocent dissemination;⁴⁴ and even a Cyber-court.⁴⁵

1 Self-regulation

The most avid users of the Internet would like the law to stay outside of their domain, leaving the people who best comprehend it, namely users, to solve their own quandaries. Legislation is seen as an unworkable onslaught into the core principles underlying the Internet, specifically freedom of expression and open, unregulated discussion of ideas.

⁴² See for example, above n 5,

⁴³ Above n 5.

⁴⁴ See the draft UK "Defamation (Responsibility for Publication) Bill" in Dooley above n 31, 47 (attached as Appendix I).

⁴⁵ See, for example, discussion in Peter Bartlett "Internet - the legal tangle" (1995) 11 Computer Law & Practice 110.

The advent of mobile telephones was such a novelty that, at the time, no one seemed to mind how or when they were used. Today, these devices are a part of normal life and their novelty value has been replaced by concerns for their use. For example, a rudimentary form of mobile phone etiquette is developing which makes society frown on their use on public transport, in movie theatres or at restaurants where their use can annoy and disturb others. Similarly, on the Internet there is a form of "netiquette" or protocols to which the Internet community subscribes governing how users interact with the system and each other.⁴⁶

Extending this unwritten code of conduct into the area of defamation might mean that if a user was found to be in breach of "netiquette", then they may be greeted with a barrage of "flames" (copious amounts of ungracious replies). In addition to this, and perhaps a more expedient approach, is vindication through the Internet forum itself in the form of a right of reply. While certainly a more cost effective way in which to settle the conflict, there remains the risk that defamation can cause real and significant damage to the reputation and livelihood of innocent people. It may be that a law suit is the only practical means of counteracting this level of harm.⁴⁷

Further to arguments of self-regulation, it has been suggested that a "Cyber-Court" could be established to govern disputes on the Internet and incorporated into the Internet structure.⁴⁸ Despite sparse literature available on the concept and the fact that the logistics have not been thoroughly worked through; the idea of a "Cyber-Court" on the Internet as a non-legal forum for adversaries to resolve their differences in the short term, has been mooted mostly by those in favour of self-regulation and would probably entail redressing electronic defamation via the same delivery mechanism in the form of published electronic apologies. While it may seem this idea is a logical progression for the Internet, is cost effective and addresses jurisdictional issues; a "Cyber-Court" is not an appropriate way to deal with controversy involving the rapidly expansion of

⁴⁶ Not using capital letters in communications on the Internet is an example of this type of rule - capital letters denote SHOUTING at someone.

⁴⁷ A further issue on this point, yet beyond the scope of this paper, is whether it is a person's actual personality or merely one's cyber-personality that is harmed by defamation on the Internet; or is there even a difference between the two?

⁴⁸ Above n 45, 112.

mainstream methods of communication and might best be reserved as a non-legal way of dealing with smaller one-on-one squabbles. First, the right to an untarnished reputation has considerable value attached to it by society. The transfer of such matters to be challenged in a forum other than a traditional legal one is unlikely to be tolerated by those who highly regard their reputations as important and of great weight. Secondly, it is unlikely that Judges would be willing to relinquish their jurisdiction in such a manner and possibly open the door to future indifference to the law in case this should occur with other legal matters.

While self-regulation may be useful, it is only likely to be beneficial to a limited degree because self-regulation of the Internet is unlikely to be able to adequately rectify or vindicate genuine grievances of innocent people who have been unjustifiably harmed. As a result, self-regulation could be deemed as having little, if any, meaning in the defamation and Internet context.

2 *A new tort of defamation*

Having discussed earlier in this paper that existing defamation legislation is not an appropriate way of dealing with Internet defamation, it could be that a new common law tort of defamation relating specifically to the Internet is a possible option for reform. Difficulties between the *Prodigy* and *CompuServe* decisions relating to the exercise of editorial control and exoneration from liability would first have to be overcome. In addition, if defamation on the Internet was to become a new common law tort, it would be a challenge for those involved in its development to reconcile two competing interests. First, there is the public interest in providing redress for someone who has suffered an injustice by being the subject of defamatory material; and, the acceptance and aims of the Internet as a means of ensuring freedom of expression and openness in the exchange of information and ideas. Placing the balance too far in either direction creates problems in terms of failing to protect the reputations of innocent people and, on the other hand, breaching s14 of the Bill of Rights Act.

3 *Defamation legislation encompassing the Internet*

Given increased advances in technology, a clause amending the defence of innocent dissemination similar to that proposed in the United Kingdom might also be useful in New Zealand by specifically referring to defamatory statements published by electronic means.⁴⁹ In line with the *Thompson* case, this defence would not offer hands-off immunity to ISPs and would not, therefore, protect those who have cause to know they are publishing defamatory material. As noted by Dooley,⁵⁰ the draft Bill encourages sensible use of the Internet by individual users and ISPs without conferring the obligation to monitor. To absolve themselves from liability the draft Bill would require ISPs to show they were not negligent in their operations and they further had no knowledge of the existence of defamatory content.

It is questionable whether domestic legislation would be an effective remedy for defamation given the Internet's borderless environment and disregard for traditional legal concepts of jurisdiction. Complicating matters further is the fact that the law is typically unable to keep abreast of mundane technological advancements, let alone keep pace with the Internet's infinite development.

B *Protecting ISPs*

An initial starting point for regulating the Internet in a defamation sense is the development of a realistic and enforceable code of conduct by ISPs. This would allow the development of legislation appropriate to the current environment but remains flexible enough to embrace future changes.

⁴⁹ Above n 44.

⁵⁰ Above n 31, 47.

1 *A code of conduct*

An international uniform code of conduct adopted by all ISPs would represent a strong front as to acceptable standards on the Internet. Violation of the code of conduct, when discovered, may mean losing one's right to access the Internet or some other appropriate penalty. With open communication between service providers on the Internet, perhaps via a database, recalcitrant users could be blacklisted and may therefore have difficulty in obtaining a connection with different service providers. Liability on the part of service providers for the subsequent infractions of users might also be effective; constituting negligence by offering a service agreement to a blacklisted person in favour of their own commercial gain. While only a very basic outline of what might go into a code of conduct, a framework, not unlike that for broadcasting standards, based around these guidelines may assist in removing, or at least reducing, the incidence of defamation on the Internet. The difficulty with this, however, is that unlike codes of conduct used for broadcasting standards, ISPs are unlikely to have similar monitoring capabilities or authority.

2 *Avoiding a finding of liability for an ISP*

In addition to a code of conduct, it would be prudent for ISPs to adopt other security measures in an effort to minimise their own liability in defamation claims by identifying the original author.

Unlike traditional modes of communication, ISPs have less opportunity to review the content of material published on the Internet due to the characteristics and speed of the Internet as described earlier in this paper. The cases so far suggest that service providers may be seen as having some responsibility for defamatory material. As can be seen in the *Prodigy* decision, there may be some merit in adopting a hands-off approach but, as mentioned earlier, this may result in a finding of negligence. Instead, the best position a service provider might adopt is one between the two extremes of refusing to monitor content and proclaiming to oversee all material placed via their system. Either extreme is likely to result in a finding of liability against an ISP. A set

of guidelines should be incorporated into the suggested code of conduct with the assertion that it is the individual user's responsibility to ensure messages do not encroach on the rights of others. In further reserving the right to edit and remove defamatory material, it would be a cautious move on the part of an ISP to declare that resources can only allow for limited monitoring of messages and that severe repercussions will follow in the event a message is traced back to the original poster.

Similarly, service agreements with users and other suppliers of information should also spell out areas where the service provider does monitor and control content and accepts liability, distinguishing those areas where the service provider acts as a mere vehicle for access and will not accept liability. Service contracts should also identify individuals by names, addresses and contact details, perhaps including a traceable on-line usercode to ensure that users can be later identified by the service provider if this is required. Policy difficulties that run against this argument, however, relate to issues of privacy and the right to go about one's business without interference. Also at issue is the possibility that the use of this type of identification procedure may inhibit communications between people in the likelihood it may later be traced back to them; it is perhaps also important to remember that not everything that is anonymous is sinister.

Insurance against misuse is also essential due to sizeable damages awards that are often made in defamation cases. Home pages or other easily accessible sites should also be available on-line and state in plain language that the Internet is not to be used for the publication of defamatory material is also worthy of consideration.

Employers should also contemplate similar actions with employees if their place of business involves using the Internet. In forbidding employees to use work computers to send defamatory messages or alternatively seeking an indemnity from employees for statements made via e-mail, employers can be held as attempting to absolve themselves from liability. Essentially the employer would be showing that defamatory material which originates from the particular workplace is not the employer's responsibility because such actions are outside the authority of the employee concerned.

BIBLIOGRAPHY

While not a cure-all for eliminating defamation on the Internet, the methods described above constitute a small step in the right direction and attempt to place responsibility with individual users of the Internet as compared to service providers.

VI CONCLUSION

Liability for defamation on the Internet has not just been isolated to individuals. Corporations are liable for the actions of employees and would prove to be attractive targets for law suits due to their ability to meet the payment of damages. What can be ascertained from cases such as *CompuServe* and *Prodigy* is that users of the Internet can no longer ignore the legal implications of their actions. Like any other publishers with a potentially large audience, users must take care not to infringe the legal rights of others. If the Internet is to fulfil its potential of becoming a useful tool in society it will have to be adequately regulated. While appropriate to a certain extent in cyberspace, existing defamation law requires clarification as it applies to the Internet. While it may be appropriate that ISPs should bear some responsibility in instances where they have acted negligently or failed to exercise sufficient precaution, procedures such as the development and implementation of a code of conduct, in conjunction with clear guidelines as to user responsibility for defamatory material, insurance policies to guard against liability, employee indemnities and clear guidelines, may assist in checking against instances of defamation on the Internet. Rather than trying to "pigeonhole" instances of defamation which occur on the Internet into existing legal paradigms, New Zealand courts need to recognise that the Internet provides a unique type of service which does not always fall into the neat rules governing other information carriers such as newspapers, television and radio. While this is perhaps the best solution, it will admittedly be difficult to achieve given the dynamic and changing characteristics of the Internet.

BIBLIOGRAPHY

Articles & Texts

- Arnold-Moore, Timothy "Legal Pitfalls in Cyberspace: Defamation on Computer Networks" (1994) 5 *Journal of Law and Information Science* 165.
- Barnard, Laurette "New Zealand report on rules for declining to exercise jurisdiction in civil and commercial matters: forum non conveniens, lis pendens" (Wellington, 1994).
- Bartlett, Peter "Internet - the legal tangle" (1995) 11 *Computer Law & Practice* 110.
- Braithwaite, Nick "The Internet and bulletin board defamations" [1995] *New Law Journal* 1216.
- Davies, Clive "Law and the Internet" (1995) 11 *Computer Law & Practice* 106.
- Dicey & Morris *The Conflict of Laws* (11 ed, Stevens & Sons Ltd, London, 1987).
- Dooley, Stephen "Dealing with defamation on the internet" (1996) 140 *Solicitors Journal* 96.
- Goddard, David "Conflict of Laws - The International Element in Commerce and Litigation" (New Zealand Law Society Seminar, Wellington, 1991).
- Halsbury's Laws of England* (4 ed, Butterworths, London, 1979) vol 28, Libel and Slander.
- Halsbury's Laws of England* (4 ed reissue, Butterworths, London, 1996) vol 8(1), Conflict of Laws.
- The Laws of New Zealand* Volume 7, Conflict of Laws: Jurisdiction & Foreign Judgments (Butterworths, Wellington, 1996).
- O'Gorman, Stephen "Defamation and the Internet" *Internet Australasia* (November 1995, Volume 1, Issue 11, p 28).
- Scott-Bayfield, Julie "Defamation update" (1995) 139 *Solicitors Journal* 189.
- Siderits, Matthew C "Defamation in Cyberspace: Reconciling *Cubby, Inc v CompuServe, Inc* and *Stratton Oakmont v Prodigy Services Co*" (1996) 79 *Marquette Law Review* 1065.
- Sykes & Pryles *Australian Private International Law* (3 ed, The Law Book Company Ltd, Sydney, 1991).
- Taylor, Jeffrey M "Liability of Usenet Moderators for Defamation Published by Others: Flinging the Law of Defamation into Cyberspace" (1995) 47 *Florida Law Review* 247.
- Todd, Stephen (ed) *The Law of Torts in New Zealand* (2 ed, Brooker's Limited, Wellington, 1997).

Wells Branscomb, Anne *Who Owns Information? From Privacy to Public Access* (BasicBooks, New York, 1994).

Wiggin, Peter *Wired Kiwis: Every New Zealander's Guide to the Internet* (Shoal Bay Press, Christchurch, 1996).

Table of Cases

Cubby, Inc v CompuServe Inc (1991) 776 F Supp 135.

Mount Cook Group Ltd v Johnstone Motors Ltd [1990] 2 NZLR 488.

Rindos v Hardwick (Unreported judgment 940164, 31/3/94, Supreme Court of Western Australia, Ipp J).

Stratton Oakmont v Prodigy Services Co (1995) 23 Media L Rep 1794.

Thompson v Australian Capital Television (1994) 54 FCR 513.

Legislation

Defamation Act 1992

Internet Sources

Cumbow, Robert C & Wrenn, Gregory J "Reputation on (the) line: defamation and the Internet" <http://www.perkinscoie.com/resource/cumb026b.htm>

Eden, Eric "Libel & Defamation in the Information Age"
<http://www.english.upenn.edu/~afilreis/defm-in-cyber.html>

Johnson, Bruce E H "Hammering the Square Peg: Speculations on Defamation and the Internet" (from *First Amendment Law Letter*, Autumn 1996)
<http://www.dwt.com/TextOnly/News/firstamendnews/hammering.html>

Muth, R Timothy "Old Doctrines on a New Frontier - Defamation and Jurisdiction in Cyberspace" <http://www.rbvdr.com/lit/defame.html>.

Sim, Peter "Electronic Libel: Responsibility of BBS Operators" October 3, 1994
<http://www.mbnet.mb.ca/~psim/libel.html>

The Standard of Care for Electronic Information Providers
<http://ww.ljx.com/public/firms/satterlee/standard.html>

APPENDIX I

The *Prodigy* case is not easily distinguishable from *Auivil*. In both cases the defendant companies could, in theory, exercise editorial control over material they transmitted, and both had exercised that control in the past. In both cases, the volume of information meant that it was not possible to vet all the material transmitted. It is also important to note that the editorial function of Prodigy's 'Board Leader' only operated once the message was on the bulletin board, ie once it had been published. *Prodigy* is widely expected to be reversed in the near future.

The English position

The liability of online service providers has not been raised as an issue in the UK, but there has been considerable discussion in legal journals as to whether they are publishers of material on bulletin boards, ie they might be found liable for defamation without fault, or are innocent disseminators of the material, just as a street vendor is an innocent disseminator of the material in the newspapers he sells. The position of an innocent disseminator is equivalent to that of a distributor in the US.

Various online service providers have adopted a hands-off approach to policing their systems to ensure that they are viewed as a Cubby-style distributor or innocent disseminator rather than as a Prodigy-style publisher. This *laissez-faire* attitude can only hinder the expansion of the information superhighway and may well lead to liability for defamation rather than avoiding it.

The defence of innocent dissemination has three elements when applied to a network operator: the operator

- 1) did not know that the network/bulletin board contained the libel complained of;
- 2) did not know that material on the network or bulletin board was of a nature likely to contain libellous material; and
- 3) did not lack knowledge of 1 and 2 above because of any negligence on the operator's part. (See *Vistelly v Mudies Select Library Ltd* [1900] 2 QB 170 for the original principles.)

If an operator becomes aware that a bulletin board is likely to contain defamatory material it will not be able to use this defence. However, if an operator closes its eyes to the nature of the material on its bulletin boards or networks, it will probably not be able to escape liability. An operator which states that it does not vet material posted on its network will find it

difficult to show that it was unaware of defamatory material being posted without any negligence on its part. A service provider will be in a much better position if it clearly reserves the right to edit material which is offensive, obscene or defamatory, whilst clearly stating that its resources are such that it is possible to view only a tiny fraction of messages posted, and that it is the individual user's responsibility to ensure that messages do not infringe the provider's guidelines. (Obviously the system provider will have to have an appropriate set of guidelines.)



Had Prodigy not expressly taken on responsibility for messages appearing on its bulletin boards, the case might well have been decided differently.

The sensible solution lies between the extremes of claiming to vet all material posted and refusing to look at any of it. The adoption of either extreme as a policy is likely to result in liability for defamatory material posted on a provider's system.

Proposed new law

In July 1995 the Lord Chancellor's Department published a draft Defamation Bill reforming, amongst other areas, the defence of innocent dissemination. These reforms are in the light of advances in technology since the defence was first considered. The relevant clause reads:

1 (1) In proceedings for defamation it is a defence for a person to show that he was not primarily responsible for the publication of the statement complained of and that he did not know, and having taken all reasonable

care had no reason to suspect, that his acts involved or contributed to the publication of a statement defamatory of the Plaintiff.

(4) The following shall not be regarded for the purposes of this section as primarily responsible for the publication of a defamatory statement –

(c) in the case of a defamatory statement published by electronic means, a person involved only –

- (i) in processing, making copies of, distributing, or selling any electronic medium in or on which the statement is recorded, or**
- (ii) in operating any equipment by means of which the statement is retrieved, copied or distributed.**

The draft Bill goes on to state that, in determining whether reasonable care has been exercised, the courts are to pay attention to, amongst other things, the defendant's responsibility for the content of the statement or the decision to publish it. This will be minimal for the average service provider.

This defence is not intended to protect those who have cause to know that they are publishing defamatory material: this will include those who refuse to adopt a sensible attitude to policing their networks. Clearly no blanket immunity is intended for service providers, nor would one be appropriate. The draft Bill

encourages sensible use by individuals and sensible policing by service providers, but without imposing an obligation to censor or conferring a right to do nothing, and requires that the service provider shows that it was not responsible for the libel, had no knowledge, and was not negligent.

The draft Bill adopts the position that the transmission of a defamatory statement over a computer network amounts to libel. This agrees with the view expressed at the beginning of this article and with the US case law.

One area left open by the draft Bill is clarification on where the publication of libellous material takes place. The current position under English law is that publication occurs in the place of communication rather than creation; and a libellous e-mail message received in Swindon from a source in Stockholm will be subject to English libel laws ■

Stephen Dooley is a member of the IT Department at Morrell, Peel & Gamlen, Oxford, e-mail: mpg@ukerna.ac.uk.

A Fine According to Library Regulations is charged on Overdue Books.

VICTORIA UNIVERSITY OF WELLINGTON LIBRARY

LAW LIBRARY

VICTORIA UNIVERSITY OF WELLINGTON LIBRARY



3 7212 00542460 9

Stephen Dooley is a member of the IT Department at Mott, Peel & Gamble. Oxford, e-mail: mpeg@vama.ac.uk

The English position. The liability of online service providers has not been raised as an issue in the UK, but there has been considerable discussion in legal journals as to whether they are publishers or merely as distributors. Various online service providers have adopted a hands-off approach to policing their services to ensure that they are viewed as a Caddy-style distributor or innocent disseminator rather than as a Prodigy-style publisher. This latter view will not only limit the exposure of the information superhighway and may well lead to liability for dissemination rather than creation.

e

1

Folder

Go

Gooding, Michelle Nena

Defamation and the

Internet

