

Internet Liability Exposures and the Insurance Response

At last count there were more than 28,000 web-sites registered in New Zealand and over 137,000 Internet subscribers. Worldwide the number of people subscribing to the Internet is estimated at 43 million and growing.

This presents an opportunity for business to gain ready access to the worldwide market at a nominal cost. The growth in this new communication tool has spawned the birth and in some cases growth of the dot.com company. With this new opportunity comes the hazards associated with it. We will look at a number of the issues facing companies and individuals who transact business on the web and what the insurance industry has done to date to address these issues.

Businesses now depend upon the Internet for every aspect of their operations, including advertising, marketing, sales, communications and public relations. Technology has developed at a speed beyond what most commentators could have predicted. How has the insurance market coped with this rapid change in technology? What are the exposures, and how has the insurance industry responded to the challenge of technology?

From the early 1980's the insurance industry developed insurance products that respond to the material damage exposures of computers and computer equipment. The standard ISR policy covers the material damage to business computers and the household contents policy responds to loss or damage to the home PC. We will not spend any time on the material damage aspects of technology but rather concentrate on the liability exposures that arise from the Internet.

THE EXPOSURES THAT THE INTERNET AND MODERN COMPUTER TECHNOLOGY PRESENT TODAY.

I stress today because the only certainty in the technology world is that the goal-posts are continually changing. Today's problem will almost certainly be different in a month or a year. There is a need to continually review the exposures faced and the adequacy of the risk management methods being adopted to address those exposures. Insurance is one method however as the exposure is continually changing the adequacy of any insurance response needs to be kept in context.

What are the exposures that exist in relation to the Internet?

We believe that a majority of the Internet related claims against businesses will arise in the areas of defamation, intellectual property and the right to privacy.

Several characteristics of the Internet will enhance the impact of these traditional legal principals. For example, the speed of web communications and the wide dissemination of materials made possible by the Internet magnify traditional defamation exposures. Similarly, the ability of a computer user to make a perfect copy of a document, to make changes to it and then disseminate it widely, complicates enforcement of intellectual property rights. It has also been observed that the need to protect the privacy of clients and customers from hackers and cyber-thieves enhances the need for adequate security. In an age where personal data has value as marketing information, privacy issues also arise in the context of a company's management of data regarding customers. Companies must develop policies which adequately protect their clients' right to privacy and protect the business from claims arising from the sale or misuse of such data.

Businesses are also exposed to the risk of direct losses from hackers and cyber-thieves. The term "Cyber Warfare" has been used to refer to the use of viruses and other tactics to "malevolently attack industries, businesses, social utilities or national security with an intent to cause disruption or damage."¹ Such piracy can cause direct losses to a business, including property damage, business interruption, theft of trade secrets and damage to business reputation. Third parties may also assert claims against businesses as a result of loss and damage caused by a hacker's breach of the company's systems.

In addition to identifying the business risks arising from use of the Internet, this paper will also address the development of insurance products to meet those risks. Insurers have issued and are developing a variety of products to protect businesses with respect to the potential property damage and business losses they may suffer as a result of cyber warfare as well as their liability to third parties for the risks associated with Internet usage.

DEFAMATION

Defamation is the written (libel) or oral (slander) publication of a statement to one or more third parties which tends to harm the reputation of another. More specifically, liability for defamation is based upon the following elements:

- a. a false and defamatory statement concerning another;
- b. an unprivileged publication to a third party;
- c. fault amounting to at least negligence on the part of the publisher; and
- d. either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication.

Traditionally, if the defamatory statements are in a permanent form it will be libel. If it is not in a permanent form it will be slander. The commonly accepted view is that defamatory material published electronically will be treated by the Courts as libel. This does however ignore the fact that the Internet can transmit sound. The significance of the distinction in other jurisdictions is that to succeed in defamation in respect of slander it is necessary to prove actual financial loss, whereas no loss need be proven in respect of libel. This is not the case in New Zealand. By virtue of Section 4 of the Defamation Act it is not necessary to prove special damage in an action in defamation. This removes the distinction between slander and libel and makes New Zealand a very favourable venue to bring a defamation action by someone who has been slandered but not libelled on the Internet.

It has been said that the apparent anonymity of the Internet and the immediacy of the delivery of communications between the parties encourages the creation and distribution of defamatory material. A University of Virginia Law Professor has stated that libel on the Internet should be treated differently because "a libel on the web is more permanent in impact even though it is evanescent in form."² Other commentators have taken the position that on-line defamation should not be actionable since the victim has the opportunity to use the web for an immediate response.⁽³⁾

In the Internet context, defamation cases may be pursued against: 1) the individuals creating the defamatory material on a website or in an e-mail (the primary publishers) and 2) the Internet Service Providers ("ISP") and bulletin board operators who permit access of the defamatory material to the web.⁽⁴⁾

In general, the liability of a secondary publisher (*ie.*, the distributor of defamatory material) is limited to situations where the distributor has knowledge of the false content of the material distributed. A number of courts have grappled with the issue of whether an ISP can be liable as a publisher or as a distributor of defamatory material.

An early case held that the provider of a bulletin board is not responsible for the content of the messages posted since the electronic bulletin board was a random collection of computerised messages equivalent to the posting of a written notice on a public bulletin board.⁽⁵⁾ In *Cubby, Inc. v. CompuServe, Inc.*,⁽⁶⁾ the court held that a computer service company which provided subscribers with an electronic library of news articles published by others, was a distributor of the material and was not liable for its defamatory content since it could not be shown that the ISP knew or should have known about its false content. Where, however, an ISP establishes guidelines for the posting of messages and holds itself out to the public as controlling the content of the bulletin board messages, some courts have held that an ISP may be liable as the primary publisher of defamatory material.⁽⁷⁾ Following these decisions, and to encourage ISPs to exercise control over the content of their message boards, The US Congress included provisions in the Communications Decency Act (the "CDA") (since repealed) declaring that users and providers shall not be deemed the publishers of information provided by another "information content provider."⁽⁸⁾ In *Zeran v. America Online, Inc.*,⁽⁹⁾ the Court applied the CDA to insulate AOL from liability for damages arising from a subscriber's use of an AOL message board to place false and offensive advertisements for products. More specifically, in the aftermath of the Oklahoma City bombing, the AOL subscriber offered tee shirts which made light of the victims and provided the office number of the Zeran Corporation as the place to purchase the products. While AOL cancelled the subscriber's account, he applied for a new account under a different name and reestablished the defamatory advertisements. Zeran sought to recover from AOL for the resultant damages on the grounds that AOL was negligent in failing to remove the offensive advertisement more quickly and effectively. The court held that the CDA created a broad federal immunity for service providers with respect to claims arising from information which originated with a third party user of the service. The CDA was deemed to afford immunity even if the service provider has knowledge of the defamatory content of the material.

In another leading case, Sidney Blumenthal, an assistant to President Clinton, brought an action against the on-line gossip columnist Matt Drudge and AOL for the publication of false statements that Blumenthal had abused his spouse in the on-line Drudge Report.⁽¹⁰⁾ The court dismissed Blumenthal's action against AOL on the basis of the immunity provided to it by the CDA, even though it chastised AOL for its active promotion of Drudge as a maverick gossip columnist and his site as the source of instant gossip and rumour.⁽¹¹⁾

What is the position in New Zealand?

Under section 21 of the Defamation Act there is a defence available to any person who published defamatory material solely in the capacity of processor or distributor. In order to make out the defence the processor or

distributor must not only have been unaware that the relevant information contained or was likely to contain defamatory material, but that ignorance must not be due to any negligence on his or her own part.

In order for an ISP to be entitled to rely upon this defence in New Zealand it will need to show that it is a “processor” or “distributor” and establish the requisite lack of negligence. The New Zealand Law Commission in its Report “Electronic Commerce Part Two, A Basic Legal Framework” has recently recommended that the Defamation Act be amended to include ISP in the definition of distributor, so as to limit the liability of ISPs where they have acted merely as an innocent conduit for defamatory material.

THE RIGHT TO PRIVACY

Individuals have a common law right to the protection of their privacy. These rights preclude the unauthorised use of an individual's name or likeness in a manner, which causes injury to their dignity or reputation. The public depiction of an individual in a false light is also actionable. Similarly, individuals are protected from the disclosure of private facts that are highly offensive and are not newsworthy as well as the unreasonable intrusion into their private seclusion or zone of privacy.

From a risk management context, an entity which does business on the web must develop and implement policies and security systems to adequately protect their customers' privacy. Business must certainly protect personal information about customers from resale or piracy. In its most basic form, this includes the obligation to endeavour to make web-sites secure from hackers who seek to steal credit card account numbers.⁽¹²⁾

Businesses must also develop policies regarding their use of information voluntarily provided by their customers, such as customer e-mail addresses and information about the customers' interests and preferences which can be derived from their purchasing decisions. Additional issues are raised by the information that can be derived by website operators as a result of users' visits to the site, including the options chosen, the time spent on each page and the connections to other sites made from the host site. The capture of an individual's image on webcam could also create the potential for a claim for violation of an individual's right to privacy.⁽¹³⁾

In the age of junk mail the Internet has the potential to become the ultimate junk mail tool. Everything we do on the Internet can be recorded and the '1984' Orwellian world of big brother watching us is now a reality. How do we ensure that the effectiveness of the Internet doesn't, in itself, lead to its own downfall?

INTELLECTUAL PROPERTY

The ability of users to access material that is subject to copyright or trademark protection, to make perfect copies of the material, to convert it into a printed form, or to modify it and then widely distribute the pirated material over the web, complicates the enforcement of intellectual property rights. Evolving multimedia technologies that are improving the quality of visual and audio images will further challenge the legal system in its enforcement of intellectual property rights.⁽¹⁴⁾

Generally, infringement occurs when users obtain protected material from the Internet without the permission of the owner. For example, in the Internet context, liability may be presented when a company:

- copies material from another website and incorporates it in the design of its own website;
- uses an Internet address (domain name) which is similar to another entity's proprietary name and is alleged to dilute the value of the owner's trade name or trademark;⁽¹⁵⁾
- uses links to other web-sites which may give rise to claims by the sponsors of the competing web-sites that the links constitute an unauthorised use of their corporate logo or that the creation of a link damages their business reputation;
- establishes links to web-sites while retaining a frame from the original website which alters the appearance and presentation of material from the linked site;⁽¹⁶⁾
- uses the trademark of another company on its website without permission;
- uses the trademark of another company as part of the site's description ("meta-tag") so the site will be picked up during users' key word searches.⁽¹⁷⁾
- fails to control its employees' use and dissemination of copyrighted material over its Intranet.⁽¹⁸⁾

DIRECT LOSSES FROM CYBER WARFARE

The incidence of hackers breaking into computer systems has become a daily occurrence. The recent attack on Microsoft's own system highlights the fact that no one is immune from such attacks. This high-profile incident, in which hackers tapped some of the digital blueprints for Microsoft's future products, highlights major security holes that computer experts say plague a surprising number of Fortune 500 and Silicon valley corporations.

Some analysts are worried that it may signal a new era in which viruses- now often the hallmark of pranksters – become serious tools for professionals with corporate theft or extortion on their minds.

According to Joel de la Garza, an expert with Securify, a Silicon Valley based computer security firm, "While eighty percent of security incidents are teenage kids out to have a good time the remaining 20 percent are hackers with a stated objective and a definite plan on how to accomplish it."

The San Francisco based Computer Security Institute says nine out of ten companies and Government organisations surveyed reported security breaches in the past year. Of the 42 percent willing or able to quantify the damages and financial losses, the total ran to US \$265 million.

The risks of the loss of data, damage to company systems or theft of confidential business data are significant. A survey conducted by mi2g software⁽¹⁹⁾ concluded that it would cost a total of \$20 billion to service incidents arising from such piracy in 1999.⁽²⁰⁾

THE INSURANCE RESPONSE

How has the insurance industry responded to this new risk?

Commercial General Liability ("CGL") Policies may afford coverage for some of the traditional causes of action that may be asserted against business as a result of their use of the Internet. For example, the advertising injury clauses of CGL policies may be triggered by the alleged use of copyrighted or trademarked material in the context of the advertisement of a product or service. Advertising injury coverage may also include claims for the publication of information that violates another's right to privacy. The problem in New Zealand is that most CGL policies do not contain a coverage grant for advertising liability as is common with US policies. There also exists the problem of jurisdiction. If the CGL policy contains restrictions on the jurisdiction from which claims can be brought this may prevent any recovery under the CGL policy.

CGL policies may also afford coverage for traditional personal injury claims arising out of libellous material published on the Internet. The application of traditional business coverages to web-related activities will depend upon the specific wording at issue and policies must be read carefully to determine the scope of coverage for causes of action arising in the context of Internet operations. While the CGL policy may not include an exclusion and therefore by implication there may be coverage, it is unlikely that the Insurer will have considered the exposure when the original terms were set. The insurer will be looking for a way to avoid liability rather than looking to assist the client.

Traditional crime and fidelity insurance do not, generally, contemplate the type of losses resulting from threats posed by hackers and cyber-thieves and, as such, are inadequate to cover businesses for the attendant risks.

What specialist insurance policies exist to offer coverage for the first and third party risks arising from web-based operations? We have seen the development of Internet specific policies by a number of insurers. We will briefly highlight the policies that are available from our company St Paul International Insurance Co. Ltd. As technology develops so rapidly it is difficult to keep pace with the changes in technology and impossible to keep pace with what our competitors may be offering as solutions.

We have split the insurance product offerings into two categories, those for Technology companies and those products developed specifically for users of Technology.

Insuring Technology Companies.

Techsure: Errors and Omissions and Media liability cover for Technology companies such as software developers, integrators, facilities managers, ISP's and related services, multimedia developers, hardware manufacturers and distributors and telecommunication companies.

This policy provides broad coverage on a worldwide basis for both the negligence and the breach of copyright and defamation exposures of these companies.

Insuring Technology Users.

Networker: A product developed specifically to address the security aspects of technology. This product offers cover for: computer systems fraud, telecommunications theft, loss caused by hackers, computer viruses, business interruption, post loss security services.

Internet Liability: Covers liability arising from the ownership of web-sites and the use of e-mail. This policy specifically covers infringement of Intellectual property rights, defamation, unauthorised use of intellectual property, passing off, breach of privacy, misuse of confidential information, and unintentional transmission of a virus.

Public Key Infrastructure Solutions: errors and omissions cover for PKI vendors and security firms.

The range of covers available is growing as technology develops.

CONCLUSION

We believe that business use of the Internet and other advances in multi-media communications will continue to grow at an exponential rate. While use of the Internet for business communications, sales, advertising, and marketing will be essential for successful business operations in the next decade, businesses also need to manage the risk attendant to these operations. Businesses should implement adequate security controls and develop policies for the management of personal data and employee use of the Internet. Businesses should also work with experts to ensure that their website designs afford as much protection as possible for their own intellectual property rights without violating the rights of other entities.

While we expect that the courts will continue to apply traditional legal principles to business issues arising in the context of Internet communications, we also anticipate that Government will respond to some of the unique challenges arising from the widespread use of the Internet. We expect the enactment of legislation to protect the public by encouraging ISPs to monitor and control objectionable material on web-sites operated by their subscribers. We also believe that ISPs may be required to take action to preclude or limit the operation of sites, which contain child pornography and hate literature.

We predict that insurers will continue to develop and refine additional insurance products to assist businesses in managing the risks of doing business on the web.

End Notes:

1. *Countering the Growing Threat of Cyber Warfare and Viruses*, Hammond Suddards Information Intelligence Seminar II: Cyber Warfare, Sept. 8, 1999, at 3.
2. Delta & Matsura, *supra* note 1, § 7.03 [B] (citing John Schwartz, *Journalism's Old Rules Should Apply to Cyber-Libel*, Wash. Post, Jan. 26, 1998 (Wash. Bus. Supp.), at 20).
3. *Id.* (citing, Mike Goodwin, *Libel Law: Let It Die*, Wired, Mar. 1996, at 116, 118).
4. *Id.*
5. *It's in the Cards, Inc. v. Meneau*, 535 N.W.2d 11 (Wis. Ct. App. 1995).
6. 776 F. Supp. 135 (S.D.N.Y. 1991).
7. *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L.Rep. (BNA) 1794, 5 CCH Computer Cases 47,291 (N.Y. Sup. Ct. 1995).
8. The Communications Decency Act of 1996, 47 U.S.C. § 230, *et seq.* (1999).
9. 129 F.3d 327 (4th Cir. 1997).
10. *Blumenthal v. Drudge*, 992 F. Supp. 44 (D. D. C. 1998) .
11. *Id.*, at 51.
12. Jared Sandberg, *Losing Your Good Name on Line, All it Takes Is Your Social Security Number, and Somebody Can Steal Your Identity - and the Net's Making it Easier for the Bad Guys*, Newsweek, Sept. 20, 1999, at 56.
13. See Jennifer Tanaka, *The Whole World Is Watching - as More and More Cameras Hook up to the Net, the Web Is Growing Eyes, but Is Everyone Ready for a Close-up?*, Newsweek, Sept. 20, 1999, at 74.
14. Examples include hybrid CR-ROMs which combine the CD storage capability with web access, an expanded optical mass storage system known as a digital versatile disk ("DVD"), digital photography, and a portable digital audio player known such as the "Rio" which has given rise to fears of increased music piracy. Delta & Matsura, *supra* note 1, § 5.02 [B] [12].
15. Since 1992, commercial domain names have been registered with a non-profit entity, Network Solutions, Inc. ("NSI"). NSI registers domain names on a first come, first serve basis. An entity may challenge the use of a domain name as a violation of a pre-existing trademark. Delta & Matsura, *supra* note 1, § 5.04 [B]. Registration practices have given rise to the sale of registered names. Hillary Clinton reportedly paid \$6,000 for the right to use the domain name "hillary2000.com" and an individual who registered the domain name "gwbush.com" is using the site to spoof the Bush presidential campaign after the candidate's organization refused his offer to purchase the site for \$350,000. *The Mouse that Roars, A Cyberguerilla Takes Shots at the Bush Camp*, Newsweek, Sept. 20, 1999, at 53.
16. Delta & Matsura, *supra* note 1, § 5.02 [B][7].
17. *Id.*, § 5.04 [B][2].
18. *Id.*, § 5.02 [B][10].
19. A London-based company, mi2g software specializes in the provision of high-security software applications for corporations and financial institutions.
20. *Countering the Growing Threat of Cber Warfare and Viruses*, Hammond Suddards Information Intelligence Seminar II: Cyber Warfare (Sept. 8, 1999), at 3.