November 1997

Email liability: postcards from the edge

Jay Forder
Bond University, jay_forder@bond.edu.au

Patrick Quirk
Bond University

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Recommended Citation
Jay Forder and Patrick Quirk. (1997) “Email liability: postcards from the edge”.


This Journal Article is brought to you by the Faculty of Law at ePublications@bond. It has been accepted for inclusion in Law Faculty Publications by an authorized administrator of ePublications@bond. For more information, please contact Bond University’s Repository Coordinator.
Is an e-mail as private as a phone call or as public as a postcard? What are the legal implications of the wide use of this medium in the coming age of telecommuting?

For some reason, when one compares "snail" mail with "e-mail", the latter seems far more dangerous. Sources of concern include:

- on-line defamation and tortious liability (including employer's vicarious liability for acts of employees; consider also "innocent dissemination" defences discussed below);
- sexual harassment and discrimination laws;
- privacy laws (especially as they relate to employees);
- legal professional privilege and security issues (could a lawyer be liable in negligence for failure to encrypt an e-mail sent to a client?);
- consumer protection laws (e.g., the ubiquitous section 52 of the TPA);
- contracts entered into on-line;
- obscenity laws;
- copyright and trade mark breaches;
- the law of confidentiality and trade secrets (people appear far less inhibited when communicating by e-mail – this may stem from the (wrong) assumption that it is a "fleeting" or "non-permanent" form of communication).

Less obvious sources of liability might include:

- on-line stockbrokers coercing clients by e-mail;
- on-line stalking;
- industrial relations law (e.g., use of e-mail by union organisers);
- unauthorised monitoring of e-mail;
- "harvesting" of e-mail addresses and the on-sale of accumulated address lists without permission;
- e-mail forgery and the "anonymous remailer" problem;
- defamation and copyright liability when framing/inlining/linking to an e-mail address or WWW site.

Doubtless there are others and the potential for conflict between various types of liability is also emerging. For example, could an ISP be liable for copyright infringement if they fail to remove an offending BBS post, and yet remain liable in defamation for actually removing the same post? There was a time, prior to section 230 of the US Telecommunications Act 1996, when this was a real danger in some US jurisdictions. The reason for this incongruity was that removal implied a level of content control and control is a governing factor in the "publication" requirement of defamation.

The relationship between a potential defendant and an offending e-mail post is also replete with possibilities. Liability may vary depending on the following factors:

- whether you own the network where the e-mail is published;
- who is to provide content to place
on the network and upon what terms (express or implied);
- whether you are a "service" or "access" provider;
- whether you are the employee of someone who owns or makes use of a network;
- whether there are adequate safeguards over the network, such as password protection;
- whether staff have been properly trained in the company's e-mail policy;
- the degree of control the network owner has or professes to have over the content of the system.

Let us look at two of the issues raised. Firstly, when might owners of computer networks be liable for defamatory material placed on their system? Secondly, under what circumstances may e-mail be "monitored" in order to detect such material?

1. When is the network owner caught as publisher of defamatory material?

The answer to this question has not yet been the subject of case law in Australia, though following Rindos v Hardwicke there is no doubt that one can in fact defame over a network. So far as television is concerned, High Court dicta in Thompson v Australian Capital Television Pty Ltd & Ors confirm that the defence of innocent dissemination certainly applies in the context of modern broadcasting and may well apply in cyberspace. The majority was of the view that "There is no reason in principle why a mere distributor of electronic material should not be able to rely upon the defence of innocent dissemination if the circumstances so permit."

This defence is not unlike that which was applied in the now well known US case of Cubby v Compuserve in which Compuserve evaded liability for defamatory material which was uploaded onto their "Money Talk" computer bulletin board. The key difference between the two cases was the level of control professed by the defendants and in Prodigy's case this included the following:

- promotion of the site as "family oriented"
- content guidelines in which Prodigy manifested their intention to remove insulting and bad taste material
- automatic screening software for bad language
- "Board Leaders" who supervised various discussion groups
- an "emergency delete" facility.

Liability thus appeared to be linked directly to the level of content control and so network owners were deterred from monitoring or promoting their sites as "safe", "monitored" or "family oriented". Section 230(1)(c) of the US Telecommunications Act 1996 (the "Good Samaritan" provision) was enacted to solve the problems arising out of the Stratton decision. The section provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information provider".

Since the section came into force the view has been expressed that it does not go far enough as it fails to fully protect distributors of defamatory material (though it clearly protects publishers). However in the recent case of Kenneth M Zeran v America Online Inc ("AOL") the Good Samaritan provisions were held to protect America Online Inc from suit by a Mr Zeran alleging negligent distribution of defamatory material. Mr Zeran was the subject of a malicious hoax by an AOL subscriber who posted notices to AOL's "bulletin board" glorifying the Oklahoma bombing and then affixing Zeran's name and telephone number to the offending posts. Zeran was not himself a subscriber to AOL and suffered a barrage of threatening phone calls and public ridicule because of the hoax. Zeran's claim was rejected because his "negligence" cause of action "conflicts with both the express language and the purposes of the Telecommunications Act (per Ellis J, March 21, 1997)."

The Australian position remains unclear. A wise network owner should ensure that anyone who uses their system is aware of potential liability (including contractual obligations). This is usually done by means of a clear e-mail policy. It may be time to consider a "Good Samaritan" type law for Australia or a codification of the innocent dissemination defence, as has been attempted in the UK. An alternative would be insurance against potential loss. In all events, network owners should be in a position to identify at all times those persons who are using their system (lie name and telephone number as a minimum).

2. Monitoring e-mail

Are you allowed to monitor the messages on an e-mail system under your control? If so, should you monitor them? The question is not only relevant for service providers, but also for employers who provide e-mail at work.

There have been a number of cases on this subject in the USA. Despite the recognition of privacy rights at common law in most US States, and Congress passing the Electronic Communications Privacy Act 1986 (which prohibits unauthorised interception of e-mail), decisions favour the employer's right to monitor. But the most recent case also seems to recognise that it would be too onerous to expect employers to monitor e-mail constantly. Employees had circulated a racially offensive joke by e-mail, and the employer was held not liable for discrimination or providing a hostile work environment.

In Australia a general privacy right has not been recognised at common law and the Constitution is silent on the matter. It is not exactly clear to what extent the provisions of the Telecommunications (Interception) Act 1979 (Cth) (the "Act" or "Interception Act") apply. With increasing usage of e-mail in the work environment, it is surprising that there has been no call for judicial clarification.

The Telecommunications (Interception) Act 1979 (Cth)

The Act was intended to extend to non-telephonic messages such as telegrams and faxes. Thus a "communication" is defined to include a message, or part of a message, in data or text form.
Although e-mail was not contemplated by legislators at the time, the Act was intended to cover non-telephonic messages such as telegrams and faxes. A “communication” is defined to include a message, or part of a message, in data or text form. This definition obviously embraces e-mail.

The prohibition against intercepting is in s 7, which also specifies circumstances in which interception is permissible, such as during installation or maintenance, or under a warrant. An interception: “... consists of listening to or recording, by any means, ... a communication in its passage over that telecommunications system without the knowledge of the person making the communication.”

It is interesting to note that reading an e-mail message is not a requirement — the prohibition is against the act of recording (making a copy by means of the interception). Three other issues arise.

1. The meaning of “telecommunications system”

The recording must occur during the passage of the communication over the system. The Act defines telecommunications system as a network, including “equipment, a line or other facility” connected to the network. Messages passing through a server en route to their destination are clearly passing over the system. Messages stored on the host machine of the destination e-mail address also appear to be passing over the system, at least until opened by the addressee. It is arguable that once opened by the addressee they are no longer passing over the system, since the link is complete. They are being stored. Recording or copying at this stage would probably not be an interception.

2. The role of knowledge

If the person making the communication (in the case of e-mail, presumably the sender) knows of the recording, it is not an interception for the purposes of the Act. In some work environments employees are shown or required to acknowledge an e-mail policy. This usually occurs only once, i.e when the user is given access to the system. Many policies contain a general notification that e-mail is not private, or that the employer reserves the right to monitor. Does this imply that the employer will monitor? Is a blanket implication like this sufficient to count as knowledge, or must the sender be warned more frequently, perhaps even every time an interception is to occur? It is clear from the wording of the section that consent of the employee is not required. But it is unclear how specific one needs to be in imparting knowledge that messages will be intercepted.

3. The scope of the Act

There is an even more important grey area. It is possible that the Act only applies to public networks. If so, it has no effect on inter-office e-mail, at least as long as the message doesn’t come into contact with a public network. This would mean that there is no restriction on an employer’s right to monitor internal e-mail.

The argument might go like this: The interception provisions were originally in the Telecommunications Act. They were separated from it when the Interception Act was passed in 1979. Many of the definitions in the Interception Act (such as “telecommunications network”) are closely related to those in the Telecommunications Act. In fact some definitions (such as a “line” or “facility”) are now defined to be the same as those in the Telecommunications Act, and the issue whether “equipment, or a line or other facility, is connected to a telecommunications network” is now expressly to be determined in the same manner as the Telecommunications Act.

There is obviously a close relationship between the two Acts. The Telecommunications Act was (and still is) designed to regulate public carriers. If, in the context of the Telecommunications Act, the definition of a network must be taken to refer to public systems and networks, then it is arguable that the definition in the Interception Act should be interpreted in the same way.

Conclusions

The unsatisfactory position seems to be this:

- If you monitor ... the degree of control you exercise might render you liable for content.