

Email Abuse

Noric Dilanchian & David Currie

Email is cheap, fast and user friendly. Misuse of it is equally remarkable – it can destroy a business.

In a court case years of stored email can be scrutinised. At this point, deletion is not an option, as recently highlighted by evidence shredding in the Enron bankruptcy.

Companies as astute as Microsoft, Norwich Union Healthcare, and Telstra have fallen victim to the dangers of unwise emails or poor email management. Email abuse is widespread. In every litigation matter in which our firm has been involved there has been “smoking gun” emails.

Abuse can involve rash statements by writers who forget they are producing recorded communication. The ease, satisfaction and immediate hit of email, lulls emailers into treating email like a telephone call. As the market take off of mobile phones, chat rooms and SMS messaging illustrate, people like to talk. It takes some more training to learn to write well.

Abuse also involves lack of understanding of the purpose of certain email features, eg:

- "Reply All": Replying may not be sensible. In one instance our client received a reply containing a chain email with the full legal advice received by the other side.
- "cc": For each person you cc, first engage your brain and question whether they need to know.

Lack of training leads to poor communication. This has negative business and legal consequences. A common error is that writers leave out vital details. Yes email can be almost as instant as a face to face conversation or a phone call, but there is also a lot missing, eg the modulation of aural volume, tone, and emphasis, let alone facial expressions and body language. In business, the sketchy notes of an email abuser, are at best Clayton's communication, and at worst a secret tape recording in a confessional.

Email abusers face their judgement day in court when their “smoking guns” are exposed. Saying then that “it was just a quick email” will not go far with the judge in

court. If you send in haste, you'll regret at your leisure. In a court hearing a hasty email could be poured over for hours or days, each word interpreted and deconstructed. Sitting in court you'll stew with guilt over all the things you could have, should have, but didn't say or do before you clicked “send”.

To break the habits of email abusers your organisation needs to adopt new practices. Recognise that it's **written communication**, don't permit employees to *always* treat it as a verbal chat or **conversation**. Since email is excellent for quick notes, mouthing off and sending off is OK sometimes, but judicious use is best at all times.

Employees, companies and company directors can be individually held accountable under the laws relevant to negligence, confidentiality, defamation, anti-discrimination, intellectual property and now privacy.

Here are six examples of problems that can arise.

1. Carelessly providing incorrect advice or information which is acted upon could make salesmen, local government bodies, stockbrokers, franchisors and others who profess expertise or special knowledge liable for negligence.
2. Failure to add the phrase “confidential”, “commercial-in-confidence” or “private and confidential” can lose protection over valuable information. Your organisation's invaluable intellectual assets which have taken years to carefully develop can be shared free of charge in an email list within minutes. As recent media reports have highlighted, second hand PCs are being auctioned with hard disks full of undeleted confidential or private email records.
3. Demeaning, uncivil or abusive statements, attacking individuals or organisations, could trigger a defamation action, with the law treating such an email as a communication which is likely to cause the “ordinary reasonable member of the community to think less of the plaintiff, or to shun or avoid the plaintiff”. Defamation has been found in communications suggesting “unchastity in a woman”, disparaging a person's business acumen,

and saying someone has benefited from fraud, blackmail or other crime.

4. Racial slurs, unwanted affections from co-workers, office pranks involving emailing risqué nudity, and other material which may give offence are increasingly forming the basis for employment law claims. Employers are duty bound to exercise care over the well being of their employees. Not knowing of workplace abuse is no defence or a poor defence for employers.
5. Forwarding an attachment or a computer program, without checking whether you are entitled to, could land you and your company in a piracy or infringement case under the *Copyright Act 1968 (Cth)*. This is sure to get you media coverage, of the wrong sort.
6. Spam, eg unsolicited emails such as advertisements sent to a large number of recipients, could prompt action under the *Privacy Act 1988 (Cth)* including compensation demands by the Privacy Commissioner. Email marketing should be sent to existing customers and others who opt-in, ie consent to receive such messages.

The ubiquity of contracts in business makes one of our favourite examples of abuse - failures in contract management. We regularly advise regarding emails which have made damaging admissions and misleading representations which are liable under the *Trade Practices Act 1974 (Cth)*. There are also instances of contract breach arising from complete ignorance - a contract for the supply of goods breached because everyone forgot about it, the email was left on a PC by a former employee under a personal password.

A contract is not dependent on one piece of "paper". It can be formed in a phone call, via an email exchange, or in any combination of these and other ways. Clearly employees need proper legal communication training to ensure good contract management.

Recognition of these legal risks leads to another key principle - the benefits of proactivity.

It is safer, quicker and cheaper to reform email abusers before damage is done, than to defend legal claims and attend to a public relations disaster. There are solutions to minimise the risks.

The key message here is - give a similar level of formality to email as is given to letters.

The torment of judgement day can be avoided by implementing simple procedures. It is surprising how long it is taking for the cost of the high level of abuse currently in process to be appreciated. Just as the reduction of drink driving required building community concern and awareness, so too does the reduction of email abuse.

For the road ahead, employees need reminders that email is a means of written communication. In the commercial arena, uncertainty and ambiguity can be enemies of communication. In the legal arena they are positively dangerous.

There is a lot to learn in email reform school from the habits of good traditional letter writers. Good letters communicate well. They do this with proper spelling, grammar, punctuation and paragraphing, as well as a descriptive subject matter header, and correct identification of the names and affiliations of the recipients.

In heavy email abuse all these rules are broken. Abusers engage in chain emails; individualistic habits in spelling, grammar and punctuation; long paragraphs which join several unrelated ideas; cryptic or redundant subject headers; and the habit of sign-offs with just a first name or initials. All of this assumes that the only audience for the email will ever be the sender and the recipient. This is not the case. When other work colleagues and lawyers read this "communication", let alone explain it to a judge, it can be as unrewarding as piecing together a jigsaw with most of the board missing.

There's no problem in all this in a [social context](#), but in the business and professional arena the risks are unacceptable. Individuals can be imprisoned, organisations can lose their crown jewels, company directors can be fined personally. For trade practices breaches there are corporate fines of up to \$10 million per offence and individual fines of up to \$500,000 per offence. Under the *Privacy Act 1988 (Cth)* the fines are \$30,000 for individuals and \$150,000 for companies. Complete reform is not achievable without practical email management. In [BT Australasia Pty Ltd v State of New South Wales and Ors](#), Telstra was found to have failed to comply fully with its obligation to discover electronic data and information. Telstra had not within the required time either disclosed the existence of back-up tapes or taken any steps to restore them to determine the existence of evidence that under a court order had to be discovered (ie found and produced for examination).

Email can be sought under subpoenas, discovery orders, and applications under the *Freedom of Information Act 1983 (Cth)*. The established trend under the *Electronic Transactions Act 1999 (Cth)* is to treat online and offline written communication in most cases in exactly the same way.

Your organisation's email management system should include a policy for storing emails just as you would other documents. Some emails should be kept forever, for example those relating to the creation or ownership of intellectual property. In litigation email records can provide a silver bullet. The failure to keep them can rob a party of a defence or a basis for commencing proceedings. *The Limitation Act 1969 (NSW)* permits commencement of legal action within 6 years for a cause of action founded on tort or contract law. Accordingly emails relating to contracts should be kept for at least this period. If the contract is a deed (a type of formal contract) the limit is 12 years.

Email has become pervasive in Australian business and with it email abuse. Although the impact of the Web has been phenomenal, a [report](#) in 2000 by the University of California, Berkeley's School of Information Management and Systems estimated that world-wide about 610 billion emails are sent per year, compared to 2.1 billion static Web pages.

Lawyers are in a position to provide useful risk minimisation materials to companies wishing to reform their email abusers. The recommended reform school programme involves a healthy dose of training. Highly recommended for every organisation are:

1. **contracting and documentation** for employees and contractors, to integrate obligations under contracts, procedure manuals and business processes;
2. **email policies** - incorporate these into policy and procedure manuals dealing with use of IT overall (these should refer to compliance with standards and law, such as trade practices law);
3. **legal communication training**, including for correspondence and contracts;
4. **knowledge management** methodology incorporating document and email management (eg employees need to have an outline of the material which must not be sent externally and the back-up and other record-keeping systems);
5. **disclaimers and other legal notices**, for email, Web sites and other publications;
6. **house style manuals** to standardise the form and content of legal correspondence and

documentation, eg notices on proposals and tender bids; and

7. **email templates** automatically including the sender's name and contact details.

Failure to implement these mechanisms will keep litigation lawyers among the few beneficiaries of email abuse. Contact us for a conversation on how we can provide customised solutions for your organisation to minimise the risks of email abuse.

Implementation will lead to graduation from reform school, with a diploma bearing the school's motto: "email well and business prospers".

Suggested Areas for a Legal Audit

Email abuse is not just an IT security or employee monitoring issue.

To minimise legal claims, you should carefully consider whether the assistance of lawyers is required to draft or check documents such as compliance manuals, website legal notices, disclaimers, privacy notices, employee contracts, and trading terms and conditions.

Additionally lawyers should assist you to prepare and implement document management strategies containing guidelines on the creation, distribution and storage of documents. These should integrate with your organisation's content and knowledge management needs. Style manuals are also required to improve communication by standardising the look and content of your correspondence and documents.

These services ensure the best evidence is available to demonstrate, if the need arises, that your organisation, its employees and directors have complied with their legal obligations, and to empower your organisation to enforce legal rights and remedies against others.

The **outcome** of this recommended approach will resolve issues highlighted in the accompanying article and others in the Dilanchian E-commerce Legal Risk Minimisation Series.

Relevant Dilanchian Solutions

Dilanchian Solutions relevant to this article:

- IT & E-commerce
- Human Resources (Employees & Contractors)
- Deal Making & Contract Management
- Intellectual Property Asset Management

Dilanchian Lawyers & Consultants

The University Centre

210 Clarence Street

Sydney NSW 2000 Australia

Tel (+61 2) 9269 0229

Email info@dilanchian.com.au

For more papers visit www.dilanchian.com.au