

MANAGING YOUR ELECTRONIC INFORMATION TO REDUCE LEGAL RISKS

Why should you care?

Your business generates large volumes of electronic information every day. If it is not properly identified, organised and stored, information in diverse formats will end up stored in all kinds of medium such as laptops, hard drives, blackberries, palm pilots, mobile phones and network drives. Failure to manage electronic information can render it impossible for anyone other than the author to know that the information exists – until it's too late.

Think about the **electronic footprint** that you have left behind today: emails, documents created and printed, various changes to documents, voice mails recorded, letters, facsimiles, dictations, website forums, items stored on a USB, appointments recorded on your email software or mobile phone and text messages.

Information is one of a business's greatest assets. Failing to adequately manage it may mean that a business cannot readily access its corporate memory. This can not only devalue the business but may also expose the business when it is required to retrieve information for a client, a litigant or a statutory body.

What is the exposure?

Consider the experience of the parties involved in *Seven Network Limited v News Limited* [2007] FCA 1062 (27 July 2007) decided earlier this year. In his judgment Justice Sackville of the Federal Court of Australia said,

“The case is an example of what is best described as ‘*mega-litigation*’. By that expression, I mean civil litigation, usually involving multiple and separately represented parties, that consumes many months of court time and generates vast quantities of documentation in paper or electronic form. ... The trial lasted for 120 hearing days and took place in an electronic courtroom. Electronic trials have many advantages, but reducing the amount of documentation produced or relied on by the parties is not one of them.”

When reading that last sentence, consider that on 30 July 2007 the Supreme Court of New South Wales introduced a new practice note providing that all discovery in its commercial, technology and construction lists “is to be made electronically”, unless the parties agree otherwise.

In the *Seven Network* case, the outcome of the discovery and production processes was an electronic database containing 85653 documents comprising 589,392 pages. Ultimately, Justice Sackville admitted 12,849 documents into evidence, comprising 115,586 pages. The transcript of the trial is 9,530 pages in length. The judgment is about 1120 pages in length. One need not have in depth experience of court procedures to appreciate that the legal and administrative costs for document production alone in this case were significant.

Justice Sackville estimated that the parties had spent in the order of \$200 million on legal costs during the proceedings. Furthermore, His Honour suggested that such costs were unacceptable

and said that, “the expenditure of \$200 million (and counting) on a single piece of litigation is not only extraordinarily wasteful, but borders on the scandalous”.

E-discovery

We will hear a lot more of this term in the court system. What is it? *All the processes put in place to access, review and exchange the electronic information that is relevant to a fact in issue in a dispute and is required to be discovered.* It is not simply producing documents in an electronic form (eg. scanning hard copies into a pdf format) and tries to also capture production of information in its original “native” electronic format. The courts are trying to avoid a situation where parties are required to produce reams of paper in response to an order for discovery.

When a business is faced with orders for discovery it quickly becomes apparent that a lack of information management is a significant risk facing business today. The e-discovery process to be used by parties to litigation will depend on how the electronic information has been created, maintained and archived (as opposed to “back-ups” which are not particularly useful in the discovery process).

An order for discovery will still be phrased as an order to discover “documents” within the specified categories. Under the *Evidence Act 1995* (Cth) “document” means **any record of information**, and includes:

- (a) anything on which there is writing; or
- (b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or
- (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or
- (d) a map, plan, drawing or photograph.

A reference to a document includes a reference to any part of the document or any copy of the document.

Discovery rules

A document must be discovered if it is “relevant to a fact in issue”. A “fact in issue” is a material allegation relating to the substance of the dispute. A document is relevant to a fact in issue if it has the capacity to rationally affect the assessment of the probability of the existence of a fact, regardless of whether the document would be admissible in evidence. So what does this mean in practice?

The test for what is “discoverable” is very wide. The courts have been reluctant to restrict discovery and accordingly a document may be relevant to a fact in issue if it would tend to “throw light on” the matters in dispute. This question must be considered in the circumstances of each case and each document – there is no blanket rule.

If a record of information exists it will be susceptible to discovery processes and may ultimately be admitted into evidence in court. Consider the emails and text messages you and your colleagues may have sent and received this week. Would you be concerned were any of those to

be read out in open court? It is a good hypothetical question to ask before clicking the “reply all” or the “send” buttons.

Document storage and retention

Current communications are informal (off the cuff remarks with no thought of the ramifications), persistent (difficult to completely erase), dynamic (easily changed both intentionally and inadvertently) and disorganised (found in unexpected places). Businesses would be better placed if they could identify and control communications, or at least know what communications exist and manage them, rather than risk someone else discovering the “smoking gun” first.

Widespread destruction of documents is rarely the best policy. Disputes are rarely over official records and documents, they are generally over some misunderstanding or disagreement caused by an informal type of communication that one party believes has altered the legal relationship. If your position is supported by documentary evidence, you are more likely to prevail in court. Accordingly, retention of the right documents is essential.

Consider the following in relation to your business’s document retention policy:-

1. You may need to comply with statutory regulations regarding retention and storage of certain documents. For example:-
 - (a) Section 286(2) of the *Corporations Act 2001* (Cth) provides that a company must retain accounting records for 7 years *after the transactions covered by the records are completed* (ie. not 7 years from when the documents was created);
 - (b) Section 289 of the *Corporations Act 2001* (Cth) provides that a company may decide where to store its documents, but if stored outside Australia the company must give notice to ASIC. A local ability to retrieve is not sufficient. If your business’s information is stored on a server outside of Australia and you have not notified ASIC, you may be in breach of this provision;
 - (c) Section 262A of the *Income Tax Assessment Act 1936* (Cth) provides that records must be “readily accessible and convertible into writing in the English language” and kept for a period 5 years “after those records were prepared or obtained, or the completion of the transactions or acts to which those records relate, whichever is the later”; and
 - (d) Section 12 of the *Electronic Transactions Act 1999* (Cth) provides that information stored in electronic form must be “readily accessible so as to be usable for subsequent reference” and the method of generating the electronic form of the document must provide a reliable means of assuring the maintenance of the integrity of the information contained in the document.
2. Electronic files require specialist handling otherwise the business risks inadvertently changing, destroying or altering the information or evidence that you are required to maintain or produce.
3. Review your storage medium annually. How will you store documents? Will you be able to access the information with that media in the future? How many people do you know

who still use floppy disks or videos? In another 5 to 10 years compact discs may be obsolete.

4. It may sometimes be necessary to keep an original document. To assess this you need to consider the important aspects of that document. Does it have an original signature? Is the colour important? Is the type and composition of the document important?
5. Question whether you can slow down the volume of information that is created in your business unnecessarily.
6. Can you regulate the content of the records of information created by your employees? For example, should the business adopt an email protocol?
7. Give a thought to how you will index and classify stored information so that it is easily retrievable. Otherwise there are some different data identification software programs available. For example, there is thread identification software which can group threads of emails together so you only need to look at the top email and then consider whether you need to look at the entire thread or not.

Information management is a task often given to the most junior staff. Due to the potential exposure for your business if documents are not properly managed, information management must also be accountable to a senior staff member.

Litigation readiness

1. Analyse your business

What is your business's size, location, personnel and business type? Where are the anticipated litigation risks? Do you face litigation regularly? If so, it may be worth putting in place a comprehensive system for management of electronic information.

2. Use a multi-disciplinary approach, but have a leader

Information management is often left to IT departments and this can lead to exposure because IT is generally focused on providing hardware and software solutions rather than considering the content of the material or the legal implications of retaining or destroying information. Senior team members should be involved.

3. Write and enforce document retention and destruction policies

Your policy must consider general regulatory, tax and privacy requirements, and also any special regulations applying to your industry.

To decide whether to keep an original document consider:

- (a) What attributes of this record are critical to be kept?
- (b) Does my proposed storage method faithfully capture, store and allow reproduction of those attributes?
- (c) If not, the original must be kept.

- (d) If a statute requires retention of the original, it must be kept.
- (e) Otherwise, the electronic version will suffice.

4. **Map your systems information**

Who creates the information within your business? Consider the informal information created by your business in everyday casual communications. What is shared? Where is the information stored?

Manage your risk

Businesses should not have to operate in fear of sanction or litigation, but the reality is that management of electronic information is an essential part of working in the local and global commercial environment, both from a regulatory and a litigation perspective.

You can manage and reduce the risk of your business becoming exposed to liabilities, costs and statutory offences if you take the time to analyse your business and maintain a multi-disciplinary policy for the management of electronic information. It is critical that your policy is reviewed annually to ensure it takes account of how and why electronic information is created, shared and stored in your business during day to day operations.

Mary-Ellen Horvath
Lawyer
Truman Hoyle Lawyers
mehorvath@trumanhoyle.com.au
Tel: (02) 9226 9888
Fax: (02) 9226 9899

Truman Hoyle is a highly regarded Australian boutique law firm specialising in six complex and dynamic areas of law, being corporate, communications, technology, energy, industrial and property law. It was named Australian Law Firm of the Year (for law firms with less than 50 lawyers) at the 2006 and 2005 Australian Law Awards. The firm also specialises in providing General Counsel Services.
