

# **E-mail and litigation**

by

Stephen Mason

*Forensic & Compliance Systems Limited have been granted an exclusive license by the author to distribute this article during 2008 - 2010*

This piece is a précis of a longer article published in the *Computer Law and Security Report* during 2007

The disclosure or discovery phase of litigation in modern times tends to concentrate on the abundance of evidence available by way of e-mail communications, and there have been a number of high profile cases reported in the United States of America in particular that have illustrated the problems a party can face if it transpires that e-mails have been deleted or entire archives of back-up tapes have been destroyed or overwritten (note, this issue concerns all legal proceedings in every jurisdiction, but the cases are better reported in the United States of America). The usual response by senior management to this issue is to assume that the IT department are responsible for retaining e-mail communications. However, the IT department have no such responsibility. The IT department are, at best only the custodians of the records created by the organization: in a commercial organization, it is the company secretary who carries the legal responsibility for the preservation of business records, yet few company secretaries understand this duty.

## **Why e-mails must be preserved**

People in senior positions and at board level regularly fail to appreciate that an e-mail (for e-mail, include Instant Message) can fall into one or more categories, each of which will have to be retained for the length of time determined by law:

- a) An e-mail discussing official business between employees internally is an internal memorandum.
- b) A similar e-mail sent out to a third party relating to official business is an external communication, and should be treated as official stationery, by being sent with the same corporate information required by law that is contained on the stationery.<sup>1</sup>
- c) An extension of a telephone conversation, confirming something, for instance, is a note to be added to a file, whether it is sent to people within the organization or to external addressees, or a mix of internal and external addressees.
- d) A note to a friend to say you enjoyed the party last night is an item of private correspondence using the organization's resources. The use of e-mail for this purpose may or may not be authorized by the organization.

The types of document that have to be retained, and how long they need to be retained for, will partly depend on the nature of the business conducted by the organization. Some documents created during the course of a business are common to all organizations, whether public or private, and provisions are made in the relevant legislation for the retention of such documents. Further, public finance initiatives often have contracts that require the organization to retain all documents

---

<sup>1</sup> The Companies (Registrar, Languages and Trading Disclosures) Regulations 2006 Statutory Instrument 2006 No. 3429.

for the length of the contract (sometimes 30 years) plus seven years after the contract expires. Document retention periods are set against different criteria:

- a) Retention periods prescribed by law;
- b) Rules issued by regulatory bodies, and
- c) Industry best practice.

### **The failure to preserve e-mails**

The case of *In re Intel Corporation Microprocessor Antitrust Litigation*<sup>2</sup> is a classic example of the failure of an organization to have a proper policy in place dealing with the retention of e-mail communications. In the antitrust litigation between Intel Corporation (Intel) and Advanced Micro Devices, Inc (AMD), it transpired that Intel was not in a position to provide copies of e-mails during the discovery phase of the litigation, because large volumes of e-mails had not been preserved. A status conference took place on 5 March 2007, and in preparation for the hearing, Richard L. Horwitz sent a letter on behalf of Intel to U.S. District Court Judge Joseph Farnan Jr, explaining the issues faced by the company.<sup>3</sup> In his order dated 5 March 2007, U.S. District Court Frederick L. Cottrell, III set out the problem in broad terms:<sup>4</sup>

‘Since the last status conference, there have been troubling developments in this case. Through what appears to be a combination of gross communication failures, an illconceived plan of document retention and lackluster oversight by outside counsel, Intel has apparently allowed evidence to be destroyed. Though all the facts are not in, potentially massive amounts of email correspondence generated and received by Intel executives and employees since the filing of the lawsuit may be irretrievably lost, as may other relevant electronic documents. The damage does not appear confined to low-level or marginally important witnesses; to the contrary, Intel executives at the highest level failed to receive or to heed instructions essential for the preservation of their records, and Intel and its counsel failed to institute and police a reliable backup system as a failsafe against human error.

Intel has not yet fully assessed the magnitude of its problem, but what it has disclosed thus far demonstrates systemic evidence preservation breaches of troubling breadth and depth. Under the best of circumstances, Intel is a company that shuns creating a record of what goes on within its walls. When not under a litigation cloud, Intel automatically purges all e-mail sent or received by its employees every thirty-five days (or in the case of senior executives, every forty-five to sixty days). What backups are made are immediately overwritten the very next cycle.

Disturbingly, even after it was sued, Intel allowed this periodic destruction of its records to continue. In a half-hearted attempt at preservation, Intel instead imposed an “honor system” on selected employees, who were asked voluntarily to identify and move relevant materials to off-network storage on their personal computers. Intel also was supposed to create and retain weekly backups to deal with the inevitable lapses that infect a user-driven preservation system.’

---

<sup>2</sup> There are a substantial number of references to this case, and the reader is advised to consult a legal database, such as Westlaw, should they wish to follow this case more fully.

<sup>3</sup> Case 1:05-cv-00441-JJF Document 293 Filed 03/05/2007.

<sup>4</sup> MDL Docket No. 05-1717-JJF, Civil Action No. 05-441-JJF, US District Court (Delaware), pp 1- 2.

The learned judge then recited the problems that were uncovered at pages 2 - 3:

'Everything that could have gone wrong did go wrong. As discussed in greater detail in the balance of this memorandum, until two weeks ago, Intel failed to deliver any retention instructions to more than one-third of its 1,027 "custodians," who by definition are employees possessing "appreciable quantities" of "non-duplicative" evidence. The two-thirds who were placed on retention received faulty instructions that failed to admonish them, among other things, to save "Sent" e-mail. Other instructions were not clearly conveyed and compliance only cavalierly monitored, with the result that over half of custodians preserved incorrectly, including some of Intel's highest ranking executives who mistakenly thought "IT" would discharge their preservation obligations for them. Intel's thirty-five day e-mail "grim reaper" has relegated to the electronic dust bin the messages and attachments that custodians failed to segregate and move off-line, and for as many as half of Intel's custodians, the back-up systems that were supposed to prevent against this type of loss were never even turned on.'

In summary, Intel failed in the following ways, as set out by the learned judge on page 5:

'Intel chose to adopt and rely on a highly-risky system of document preservation. Although it has provided ever-changing descriptions of both its "normal" practices and its retention system, from that AMD can tell, Intel's preservation strategy:

Allowed the continued, automatic purge on a 35-day (or longer) schedule of all e-mail communications to, from and within the company;

Relied exclusively on a move-it-or-lose-it "honor system" that required individual custodians to correctly identify, segregate and proactively move relevant evidence to media on their local computers before that data was destroyed by a network purge;

Backstopped this "honor system" beginning in October 2005 with a weekly back-up of e-mail that required Intel's IT personnel to identify and correctly migrate custodians' data to dedicated e-mail servers subject to the backup.

As noted above, this "honor system" was defeated by a combination of apparently erroneous, unclear or incomplete "litigation hold" instructions, lack of adequate monitoring to ensure those instructions were understood and followed, and a wholesale failure timely to deliver any preservation instructions to a third of the employee-custodians Intel itself identified.'

A status conference was subsequently held on 7 March 2007 before The Honourable Vincent J. Poppiti,<sup>5</sup> in which the practical issues were discussed about how the discovery exercise was to continue. It was also agreed to appoint a neutral third party to be retained by the court to help the court determine the resolution of any future disputes of a technical nature between the parties. In addition, Intel indicated, both in the letter sent by Richard L. Horwitz before the hearing and during the course of the hearing, that it intended to buy an e-mail archiving system from a vendor with the intention of preventing the loss of e-mail correspondence in the future.

#### **The integrity of e-mails and insurance cover**

It is widely appreciated that the content of e-mails can be edited, partly deleted, and the names of the people to whom it was addressed and sent to, removed when they are sent on in the form of a

---

<sup>5</sup> MDL Docket No. 05-1717-JJF, Civil Action Nos. 05-441-JJF and 05-485-JJF, transcript of conference by Gail Inghram Verbano, shorthand reporter, [www.corbettreporting.com](http://www.corbettreporting.com).

'forward' or when replying. In this respect, the original e-mail, unless retained, is being altered. However, providing the original e-mail is retained, then the edited version does not affect the integrity of the original. However, the filing of e-mails on electronic document management systems presents its own problems. Some organizations require all relevant e-mail correspondence in relation to a particular job or client matter to be manually copied into a document management system. However, where an e-mail does not contain a suitable file reference in the subject field, for example, it is invariably the practice of employees to amend the subject field to include such a reference before the e-mail is placed into the system. If this occurs, the e-mail has been altered, and in many instances, the original e-mail as received might be deleted from the e-mail system. Naturally, the employee can also alter the content of the e-mail before adding it to the system.

It should be noted that, from the perspective of insurance cover, it is important to ensure that if an e-mail is copied into a document management system, that the e-mail (or any other form of digital document for that matter) is precisely the same as in the native file, and it is stored in such a manner that it can be demonstrated that it has not been tampered with. Should it be possible to alter any digital document before it is added to the document management system, and should it also be possible to alter any document once it is placed in the system, doubt could be cast upon the integrity of the documents held in the system, which means the integrity of such documents may be open to challenge in legal proceedings, and any insurance cover may be invalid.

#### **Some pointers that courts will consider when considering the authenticity of e-mails**

In the United States of America, partly as a result of a number of interesting cases, particularly *In re Vee Vinhnee, Debtor American Express Travel Related Services Company, Inc. v Vee Vinhnee*<sup>6</sup> and *Lorraine v Markel American Insurance Company*<sup>7</sup>, if the authenticity of any digital document, including an e-mail is raised, the party required to prove the authenticity of the document will have to adduce a range of evidence, including the following:

First, it may be necessary to demonstrate that the record is what it purports to be, and in demonstrating this, some of the pertinent points to determine whether records have been changed since their creation include:

- a) Relevant policies and procedures for the use of the equipment, database, and programs;
- b) How access to the pertinent database is controlled;
- c) How access to the specific program is controlled;
- d) How changes in the database are logged or recorded; and
- e) The structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database.

Second, proving the authenticity of a digital document requires a framework to consider how the evidence is to be assessed. This means the concepts of reliability, integrity and trustworthiness become crucial. Each of these can help provide for the authenticity. In turn, the following needs to be taken into account:

- a) The machine;
- b) Operating and Application software;

---

<sup>6</sup> 336 B.R. 437 (9th Cir. BAP 2005).

<sup>7</sup> 241 F.R.D. 534 (D. Md. 2007), 73 Fed. R. Evid. Serv. 446, 2007 WL 1300739 (D.Md May 4, 2007), 2007 ILRWeb (P&F) 1805.

- c) Storage medium;
- d) Method of retrieval;
- e) Alteration and detection of alteration; and
- f) Management of dependencies.

The evidence that comes before a court during legal proceedings reflects the way a business operates. Given that virtually every business now uses digital documents and e-mail correspondence is such vast quantities, it is crucial that the documents relied upon by the business are retained properly.

© Stephen Mason, 2008

Stephen Mason is a Visiting Research Fellow, Digital Evidence Research at the British Institute of International and Comparative Law

Stephen Mason is the author of:

*Electronic Signatures in Law* (Tottel, 2nd edn, 2007)

This text covers 99 countries and has case law from the following jurisdictions: Argentina, Australia, Brazil, Canada, China, Colombia, Czech Republic, Denmark, Dominican Republic, England & Wales, Estonia, Finland, France, Germany, Greece, Hungary, Israel, Italy, Lithuania, Switzerland and the United States of America

*E-Mail, Networks and the Internet: A Concise Guide to Compliance with the Law* (xpl publishing, 6th edn, 2006)

Stephen Mason is also the editor of:

*Digital Evidence and Electronic Signature Law Review*

*Electronic Evidence: Disclosure, Discovery & Admissibility* (LexisNexis Butterworths, 2007) (Author and Editor)

This text covers the following jurisdictions: Australia, Canada, England & Wales, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa and the United States of America

*Electronic Evidence* (British Institute of International and Comparative Law, 2008)

This text covers the following jurisdictions: Argentina, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, Norway, Poland, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland and Thailand

stephenmason@stephenmason.co.uk