Edith Cowan University
Research Online

ECU Publications Pre. 2011

2008

You've Got Mail: Accountability and End User Attitudes to Email Management.

Mark Brogan
Edith Cowan University

Susan Vreugdenburg
Edith Cowan University

This article was originally published as: Brogan, M. P., & Vreugdenburg, S. Y. (2008). You've Got Mail: Accountability and End User Attittudes to Email Management. . Proceedings of International Conference on e-Government. (pp. 63-70). RMIT University Melbourne Australia. Academic Publishing Limited.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ecuworks/1119

You've Got Mail': Accountability and End User Attitudes to Email Management

Mark Brogan and Sue Vreugdenburg
Edith Cowan University, Perth, Australia
m.brogan@ecu.edu.au

Abstract: In a pioneering ethnographic study of end user responses to the problem of 'information overload' Whittaker and Sidner (1996) found that the design of systems primarily as methods of asynchronous communication, posed significant information management problems for users. In another contemporaneous study, David Bearman (1993) extended understanding of the implications of end user email management behavior by identifying significant accountability implications for organizations arising from the use of email. Recent case studies in the United States and Australia (Leopold, 2008; Raleigh Chronicle, 2008; Strutt, and Taylor, 2007) have once again focused attention on the accountability consequences for Government of email management.

Employing elements of Whittaker and Sidner's (1996) typology, in a research design involving quantitative and case study methods, this study explores end user attitudes and behavior in email management with consequences for Australian Government accountability in an era of e-Government. The paper addresses the need of information policy makers, Chief Information Officers (CIOs) and information and records managers to be informed about current vectors in compliant email management.

Keywords: Email, archives, email management

1. Introduction

In its Technology supplement, the *New York Times* recently surveyed the implications of the Internet 'message glut' for users and employers. According to technology correspondent, Matt Richtel (Richtel, 2008):

> *A typical information worker who sits at a computer all day turns to his e-mail program more than 50 times and uses instant messaging 77 times… The fractured attention comes at a cost. In the United States, more than $650 billion a year in productivity is lost because of unnecessary interruptions.*

Message glut not only involves lost productivity, but can also affect the well being of users. The same article announced an industry alliance by Microsoft, Intel, Google and I.B.M. to fight information overload (*ibid,* p.2). But it has not been easy for major corporations and thinkers about digital communications to admit the problem. Under the umbrella of Web 2.0, in recent years Internet computing has been on social networking trajectory that emphasizes social capital i.e. the capital that attracts to a users connection to one or more social networks. Concern about 'information overload' sits uneasily with a social capital interpretation of business value and the Web.

Interest in email management has increased due to major corporate collapses, some involving allegations of fraud, malpractice and exposure through email communication. Shetty and Adibi (2005) conducted a study of the *publicly* released Enron email archive. The authors concluded that email is the most archived evidence data on interpersonal communication in electronic form allowing a comprehensive social network analysis. They noted the similarity of the Enron dataset to data collected for fraud detection or counter terrorism and that it had become a perfect test bed for testing effectives of techniques used for fraud detection and counter terrorism.

In Australia, corporate collapses such as One.Tel (2001), Ansett Australia (2001), HIH Insurance Limited (2001), and the Australian Wheat Board (AWB) scandal (2006), have similarly prompted broader consideration of the implications of business information management for corporate accountability. Business email systems have been targeted by investigators for information related to corporate and individual culpability. According to Gartner (Logan 2007, p.2) "email is the biggest driver of incremental storage costs and is frequently the target of request and subpoenas from lawyers and regulators."

2. Case study: Accountability and public sector email management

Information overload and the message glut pose problems for Government. For Government, problems posed by email include, but are not restricted to productivity and the welfare of users. They also include the vexed and contentious issue of *accountability* i.e. the principle that government decision-makers in a democracy ought to be answerable for their actions. (Bessette, 2004, p.38). But information externality caused by poor email and electronic records management more generally, negatively impacts on the efficiency and effectiveness of government accountability. In the PROFS affair of the mid 1980s, Colonel Oliver North destroyed White House email purportedly showing White House complicity in the Iran Contra affair (Wallace, 2002). The affair significantly damaged the Reagan administration and was a landmark case study in understanding how the management of messages had implications for the accountability processes of government.

In 1994, David Bearman, an American theorist on archives 'laid out the accountability significance of email' and made the observation that the problem on 'how to manage records created by electronic mail communications systems over time' would 'confront management of every contemporary organization in the next few years.' (Bearman, 1994 p.29). He also also warned of

> *"the risks being courted in organizations that use electronic mail as an informal means of communication similar to the water fountain, but don't impose strict etiquette and expectation of public release of this information. Because the record which is created is written and kept, views that would not be expressed in other documents are likely to find their way into the record with dangerous implications."*
>
> *(Bearman,1994)*

In a current case before a US District Court, *Citizens for Responsibility and Ethics in Washington v. Executive Office of the President, et al.,* a non government public interest advocacy alleged (Leopold, 2008) White House violation of the Presidential Records Act. According to the plaintiffs, White House staff had failed to archive White House emails sent and received between 2003 and 2008, including mails that related to the decision to invade Iraq. Elsewhere in the US, stung by allegations that members of his administration had violated state records law by deleting emails, the Governor of North Carolina, Mike Easley recently announced a "review of use of state owned email systems as well as electronic text communications on state owned or leased wireless devices such as Blackberry handheld units." (Raleigh Chronicle, 2008).

Concern about the management of email and its implications for accountable government is not restricted to the United States. In Australia, the WA Corruption and Crime Commission recently concluded an investigation involving email accounts of former WA Health Department, Director, Dr Neale Fong (CCC, 2008). The Commission concluded that Dr Fong made misrepresentations to his Minister, DOH staff and the media, culminating in him maintaining untruthfully in evidence before the Commission that he had no recollection of 33 email communications between himself and lobbyist Brian Burke. Digital forensic methods were used by the Commission to recover mails that had been deleted by Dr Fong.

In common with the US, the nexus between government accountability and public sector records management has attracted significant attention since the 1980s. The Fitzgerald Commission in Queensland, the Heiner Affair and the WA Inc Royal Commission (1993) were pivotal events in the establishment of statutory protections and protective machinery for government records in the interests of 'accountability'. Expert submissions emphasized the need for such protections to be fully comprehensive of electronic records and by 2000, most Australian Governments had functional recordkeeping law that encompassed the digital domain. However, unlike the US and Europe, in Australia public records management, including electronic records management attracts little funding, substantially under mining the intent of reforms to records law. Infrastructure spending varies significantly from State to State. At the time of writing only the Commonwealth and Victoria have fully functional digital archives and supporting services and infrastructure. In Western Australia, there has been no significant capital expenditure at the State Records Office since the early 1990s. Paradoxically, its records legislation is stronger than most other States.

Looking beyond Australia and the US, a recent UK Information Management industry survey that tested confidence in email archiving, reported that two-thirds of managers "have little or no confidence" that e-mails related to business decisions and obligations are "recorded, complete and

recoverable." (Dahlquist, 2008) The same survey indicated that public sector managers were less confident than their private sector counter parts. In another 2008 survey by email data management specialist C2C (McKevin, 2008), it was found the common practice of employing mailbox quotas posed problems for compliance with records legislation and that despite advances in email management software and policies, employees are still enduring mailbox quotas and are continuing to manually delete email data:

> *Overall, 65 percent of respondents have quotas and are forced to manage email manually, and 66 percent take it upon themselves to ensure their email messages aren't lost, with most storing email outside of the company email system - including in personal/home email accounts.*
>
> *This can make life extremely difficult when it comes to compliance and eDiscovery issues, particularly considering 67 percent of those surveyed needed to search for an email more than three months old at least once a month. A further 28 percent admitted to spending time searching for email about once a week or daily.*
>
> *(McKevin, 2008, p.1)*

As the C2C study suggests, organizational accountability in email management involves compliance with records law, the facilitations of e-discovery, ethical practice and other factors. More prosaically, accountability can be bound up with something so apparently trivial as a mailbox cap and how it shapes user behavior. Compliance with records legislation that extends statutory protections to records from arbitrary or malicious destruction is a core requirement for accountability. A *sine qua non* for accountability, is organizational policy that concedes the record character of some mail and the need for policy, procedures and systems that enable such mail to be captured and managed as records. Similarly, unless policy, procedure and IT systems work to facilitate the efficient discovery of records including email, accountability via administrative law (FOI) may be compromised.

3. Email and the law

Increasingly, email management behavior has become the subject of scrutiny in Australia's law courts and by regulators. In Advice 18 (2007), the Public Records Office of Victoria (PROV) responded to the case of McCabe v British American Tobacco (BAT) and in May 2006, changes to the criminal law embodied in the *Crimes (Document Destruction) Act 2006* were introduced. Mistakenly, many users do not view email as business information with the same appraisal and retention requirements as records in other formats. According to Allman (2006, p.15) "Retention decisions are thus a matter of erratic user choices or the unintentional results of IT policy decisions, such as load and storage management".

Casual and business related email conversations link business and personal worlds, so users often have difficulty distinguishing what is an official record. Depending on the habits of the user, emails may be deleted immediately after reading, or retained for years. It is not uncommon to find users with many thousands of mails kept in bloated 'Inboxes'. There are users for whom filing or deletion are seldom if ever performed. Gartner (Logan, 2007 p.2) points out that:

> *information artifacts that are 'evidence of activities' should be managed as records with business and/or legally determined destruction dates; 'read only' controls; policy driven, automatic ways to suspend routine deletion for legal hold purposes; and an expectation that when they are deleted, it is according to a defined process that is auditable, legal and beyond the reach of existing forensic technologies.*

A White Paper by MessageLabs (2008), drew attention to the fact that more than three quarters of an organisation's business-critical data is in email form. It warned against the manner in which PST files are used. Amongst the issues noted are security, inability to retrieve information and the loss of corporate knowledge when someone leaves the organization. A critical issue was the massive data back up required when several email users attach the same information into their PST folders. According to Harney (2006, pp.44, 45), a search related to legal discovery for one company was estimated as 'the cost of searching through 14 months of email back tapes (containing 20 million pages of email messages and attachments) to be in excess of $6 million and would take six months.'

4. The ECU Study

The multidimensional character of compliant email management clearly poses problems in terms of a comprehensive study of government. Hence, the ECU study discussed in this paper is very much a preliminary study and lays no claim, either to exhaustively operationalizing compliant email management, or to findings that are generalizable to government as a whole. The study is being conducted in two phases- a *pilot study* used to test and refine instruments (discussed here) and a comprehensive survey of the population proper. Results discussed here are derived from the pilot group of forty two respondents, again emphasizing the non-generalizability of findings. Other limitations of the current study are discussed below. The pilot study is reported only to illustrate methods and issues in operationalizing compliant email management.

The host government agency from which the population was drawn is a State agency that participated subject to protection of its anonymity. At the time the survey was conducted, an Enterprise Information/Content management system was in the process of being rolled out, a situation not conducive to direct measurement of end user email filing to the corporate store. In common with many other Government agencies, the agency concerned is searching for affordable, efficient solutions to the problem of compliant email management.

Unlike the C2C (2008) study which focused on deletion, searching and PST file creation, the ECU study concerns itself with two further pieces to the email puzzle- filing and archiving behavior. Two predecessor studies of end user email management behavior are significant in these terms, a pioneering ethnographic study conducted by Whittaker and Sidner (1996) and later study conducted by Microsoft (2006). The current study departs from both in using a public sector case study agency.

Measures selected from these earlier studies concern user filing behaviors, an important factor in whether record mail is captured into corporate records stores (usually achieved through Applications Program Interface (API) integration of the email client with the corporate records management system). Measures developed specifically for the current study also concern attitudes to various dimensions of email management (for example, email as a record), environment variables (e.g. email account caps) and non-filing behavior (for example, client email archiving) with audit trail consequences.

4.1 Filing

An assumption implicit in many good practice email policy and procedural guidelines, is that end users routinely and reliably file email. Where record capture to the corporate store is based on users filing mail to the store directly, or indirectly, via copying of mail folders on the client, efficient capture requires predictable filing in accordance with policy and procedure for the handling of record mail. In their study, Whittaker and Sidner (1996) found that users were uncertain about how to file email, resulting in most email being held in a 'holding pattern' while users figured out what to do with it. Where users created folders, 35% were found by Whittaker and Sidner (1996, p.280) to contain only one or two items:

> *Not only do these tiny "failed folders" not significantly reduce the complexity of the inbox, the user has the dual overheads of (a) creating them in the first place, and (b) remembering multiple definitions every time there is a decision about filing a new inbox item.*

The authors concluded that return on investment in creating folders:

> *may not be great: folders can be too large, too small or they may be too numerous for people to remember their individual definitions. As a consequence, folders may be of little use either for retrieval or viewing related messages together.*
>
> *(ibid)*

Whittaker and Sidner (1996) identified various strategies employed by users for dealing with information overload in email which they expressed in terms of behavioural types: 'No filers'; 'Spring Cleaners' & 'Frequent Filers'. 'No filers' were email users who relied upon full text searching of the inbox to find mails and typically did not file mail received; 'Frequent filers' attempted each day to reduce the size of their inbox by filing mails in folders on a regular basis; and 'Spring cleaners' dealt with overloaded in-boxes intermittently or an irregular basis.

Whittaker and Sidner (*ibid.,* p. 281) found in their sample, that 33% of email users were categorizable as 'No Filers', 39% 'Spring Cleaners' and 28% 'Frequent filers'. They also found (*ibid.,* p.282) that 'No filers' received more emails per day than spring cleaners or 'Frequent filers' and that filing behaviour appeared to be related to volume of mail received. Using inference testing, they were able to show that this result was statistically significant at the $\alpha = 0.05$ confidence level.

In the ECU pilot study group, self assessment revealed no 'No filers' with 80% of respondents (n=37) rating themselves as 'Frequent filers' and 20% 'Spring filers'. The Whittaker and Sidner (1996) finding of significant association between filing behaviour ('Spring filers', 'Frequent filers') and Inbox size was supported in 1-tailed test (n=31, rho=0.509, ρ=0.002). No significant association was identified between filing behavior and daily messages received. Similarly, Age, Gender and Job Classification showed no significant association with filing behaviour.

The volume of business mail received on a daily basis by users in the study was slightly less than Sidner & Whittaker (1996) with 77% of users reporting 40 or less mails per day. As might be expected with the majority of users experiencing low volumes of daily mail, only 14.3% considered email a source of work related stress. Investigation of the low volumes of mail received by users in the host agency revealed independent variables that explained this unexpected outcome. For example, the streaming of some mail to shared mailboxes dedicated to organizational units contributed to observed low numbers of daily messages received by individuals.

4.2 Archiving

The ECU study extended to Whittaker & Sidner's typology of user behaviour to client side archiving through the following categorization:

- 'Auto Archiver' – email users who set parameters in Outlook for auto archiving of email;
- 'Active Archiver' – email users who actively archive their email on a regular basis, but do not use AutoArchive;
- 'Inactive Archiver' – email users who never archive email using archiving functionality provided on the computer; and
- 'Spring Archiver' – email users who archive overloaded in-boxes or cabinets irregularly, or in response to an instruction from systems administrator.

Figure 1 describes the archiving behaviour of respondents:

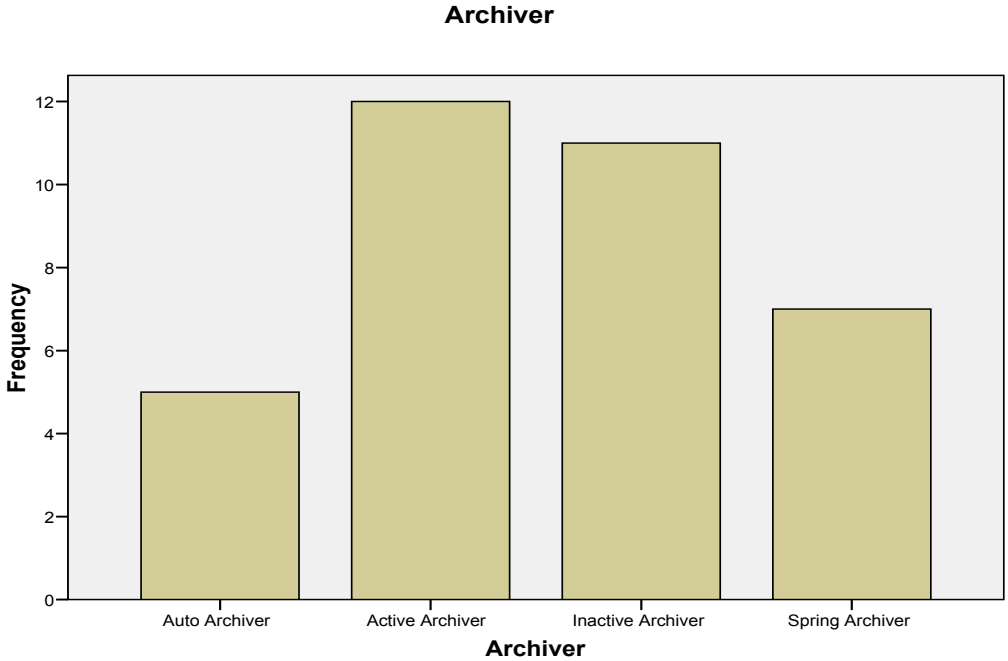

Figure 1: Bar graph of archiving behaviour

The descriptive stats showed that 73.8% of all users were involved in email archiving in some form, with only 26.2% of users considering themselves 'Inactive Archivers'. Findings are consistent with the

operation of an environment variable- a mailbox cap. The cap required users to periodically archive or delete mailbox content to stay within an allotted disk space allocation.

Archiving of email outside purpose designed archival solutions, particularly where archiving is done to a client machine, reduces information retrieval efficiency and increases the likelihood of record mail becoming lost and potentially un-recoverable. This has significant implications for e-discovery, increases organizational risk from lost and un-recoverable mail and can involve significant costs in time and resources required to find mail. In the host organization archiving appeared not to involve the client machine as the end destination, but a shared drive. No purpose designed email archiving system operated within the pilot study agency.

5. Analysis and Interpretation

Findings from the pilot study suggest different patterns of filing behaviour compared with those identified in earlier private sector studies (Whittaker and Sidner; 2006; Microsoft, 2006). Public sector users appear *more likely* to be involved in filing to user created folders than their private sector counterparts. In the pilot group, filing behavior appears not to be related to independent variables such as education, age or position. No significant association could be established between filing behavior and daily messages received.

Archiving behavior was well established in the pilot study group. Investigation revealed a system 10Mb user Inbox size limit (cap). The modest nature of this limit suggests that users would quickly exceed the system threshold and would be required to pursue either deletion or archiving as coping strategies. The host agency is by no means unique in imposing Inbox and Mailbox caps. In its 2008 Technology Survey, the Records Management Association of Australasia (RMAA) revealed that 63.6% of surveyed private and public sector organizations employ a mailbox cap.

Archiving to a shared drive improves prospects for discovery from an information retrieval standpoint, but since such drives are also used for backups and have no status in terms of the record store, the likelihood of discovery and retrieval over the long term is low.

6. Conclusion

Subject to confirmation by the larger whole of agency study, information culture suggests good possibilities for building compliance in the pilot study agency based on deployment of policy based folder disposition of mail, including replication of record mail in the corporate store. However in the pilot study agency, folder policy based disposition had not been implemented.

An acknowledged limitation of the current research, namely, that it did not measure user filing of record mail directly to the corporate recordkeeping system, is scheduled to be fixed in the full study (now underway). In the absence of such evidence, the extent of compliant or 'accountable' email management could not be measured. The widespread use of email archiving to shared drives suggests that medium term recovery of record mail not captured in the corporate store, would be problematic in the host agency.

Such a finding suggests the logic of deploying purpose designed email archiving systems that operate at gateway level as a cornerstone of compliant email management. Notably, the Corruption and Crime Commission (2008, p.86) investigation of the Fong/Burke email affair, recommended a Whole of Government (WoG) standard in relation to agencies' archival processes and retention of email communications. Since many public sector agencies are struggling to secure funding for the deployment of content and electronic recordkeeping systems, the first rung on the compliance ladder, practice may be years away from whole of government deployment of purpose designed email archiving solutions.

References

Allman, T. (2006). *Email Retention: Time for a New Approach. AIIM – The Enterprise Content Management Association ECM Toolkit (2006).* Retrieved 13 June 2008, from http://www.aiim.org/CustomerService/ViewDownloadPDF.aspx?ID=321601&PID=1725

Bearman, D. (1994) Archival Strategies. American Archivist, vol. 58, 1994, pp.374-407 Archives & Museum Informatics. Retreived 18 June 2008, from http://www.archimuse.com/publishing/archival_strategies/

Bearman, D. (1994). Managing Electronic Mail. *Archives and Manuscripts,* v.22, no.1, May 1994: (28)-50

Bearman, David (1993) The Implications of Armstrong v. The Executive Office of the President for the Archival Management of Electronic Records. In *The American Archivist* vol.56 no.4 pp.674-689

Bessette, G. (2004). *Involving the community. A guide to participatory development communication*. Ottawa: Southbound/International Development Research Council.

Business Law & Regulation (n.d.) Australian Government: The Treasury. Retrieved 24 May 2008, from http://www.treasury.gov.au/content/business_law.asp?ContentID=321&titl=Business%20Law%20%26%20Regulation

Dahlquist, D. (2008). *Confidence in Email Archiving Waning.* Retrieved 3 June, 2008, from http://www.cmswire.com/cms/enterprise-cms/confidence-in-email-archiving-waning-002427.php

Corruption and Crime Commission. (2008). *Report on the Investigation of Alleged Misconduct concerning Dr Neale Fong, Director General of the Department of Health.* Retrieved 22 March, 2008 from http://www.ccc.wa.gov.au/pdfs/report-alleged-misconduct-fong-neale.pdf

Enron Explorer, (2006). Enron. Trampoline Enron. (n.d.). Trampoline Enron Explorer from Trampoline Systems. Powered by SONAR. Copyright Trampoline Systems © 2006. Retrieved 7June 2008, from http://www.enronexplorer.com/

Fisher, D., Brush, A., Gleave, E. et. al. (2006). *Revisiting Whittaker and Sidner's "Email Overload" Ten Years Later.* Microsoft Research.

Harney, J. (2006*). TO: Corporations FROM: The Courts DATE: Yesterday SUBJECT: Email Management – Get it Now*. AIIM – The Enterprise Content Management Association ECM Toolkit. Retrieved 13 June 2008, from http://www.aiim.org/CustomerService/ViewDownloadPDF.aspx?ID=321601&PID=1725

Hazelwood. J., (2007). *Crimes (Document Destruction) Act 2006: Implications for government recordkeeping* Public Record Office, Victoria. Retrieved 24 June 2008, from http://www.prov.vic.gov.au/publications/publns/PROVRMAdvice18.pdf

Kehl, D., (2001) *HIH Insurance Group Collapse. E-Brief:* Online Only issued Date 29 November 2001 Analysis and PolicyEconomics, Commerce and Industrial Relations Group. Retrieved 8 June 2008, from http://www.aph.gov.au/library/INTGUIDE/econ/hih_insurance.htm

Large business and tax compliance. (2006). from Australian Government Australian Taxation Office Canberra August 2006 NAT 8675-08.06 JS 4584: Retrieved May 24 2008, http://www.ato.gov.au/content/downloads/77898_N8675-08-2006_w.pdf

Logan, D. (2007). *In Q&A for Information Retention Management and Records Management Tools and Services*. Gartner, Publication Date: 12 November 2007 ID Number: G00152520.

Leopold, J. (2008). *White House Official Tells Judge Searching for Lost Emails Requires Too Much Work.* Retrieved 28 March, 2008 from http://www.opednews.com/articles/genera_jason_le_080322_white_house_official.htm

McGhee, S. (2008). *Ways to Take Control of Your E-mail Inbox.* Retrieved 15 June 2008, from http://www.microsoft.com/atwork/manageinfo/email.mspx

McPhee, I. (2006). Recordkeeping including the Management of Electronic Records. The Australian National Audit Office (ANAO) The Auditor – General Audit Report Performance Audit No.6 2006-07 retrieved 9 June 2008, from www.anao.gov.au/uploads/documents/2006-07_Audit_Report_61.pdf

MessageLab (2008*). Death to PST Files: The Hidden Costs of Email.* White Paper. Retrieved 9 June 2008, from http://www.messagelabs.com/white_papers/death_to_pst

McKevin, G. (2008). Research Exposes Email Management Issues. *Image and Data Manager Online.* Retrieved 14 July 2008 from http://www.idm.net.au/story.asp?id=9724

Richtel, M. (2008). *Lost in E-Mail, Tech Firms Face Self-Made Beast.* Retrieved 15 June 2008 from http://www.nytimes.com/2008/06/14/technology/14email.html?_r=1&oref=slogin

Shetty, J., & Adibi, J. (2005). *In Discovering Important Nodes through Graph Entropy The Case of Enron Email Database.* University of Southern California, University Park, Los Angeles, USC Information Sciences Institute Marina del Rey, CA.

Records Management. (2002). Australian Standard (AS/ISO 15489) Standards Australia International ISBN 0 7337 4346 3.

Steele, K. (2006). *Good corporate conduct: exposure by email*. Retrieved 16 June 2008, from http://www.freehills.com.au/publications/publications_6231.asp

Strutt, J. and Taylor, A. (2007). McGinty Man in Burke Enquiry. *The West Australian.* June, 22 2007, p.1

The Raleigh Chronicle. (2008). *Governor Asks For Email Policy to be Reviewed.* Retrieved 28 March, 2008 from http://raleigh2.com/default.asp?sourceid=&smenu=1&twindow=&mad=&sdetail=688&wpage=1&skeyword=&sidate=&ccat=&ccatm=&restate=&restatus=&reoption=&retype=&repmin=&repmax=&rebed=&rebath=&subname=&pform=&sc=2502&hn=raleigh2&he=.com

Wallace, D. (2002). Implausible Deniability: The Politics of Documents in the Iran-Contra Affair and Its Investigations. In *Archives and the Public Good: Accountability and Records in Modern Society.* Cox, R. & Wallace D. (Eds). Westport Conneticut. Quorum Books.

Whittaker, S. and Sidner, C. (1996). Email Overload: Exploring Personal Information Management of Email. *Proceedings of the Association of Computing Machinery Conference on Computer – Human Interaction (CHI).,* 1996, 276□283.

United States District Court for the District of Columbia (2007). *Citizens for Responsibility and Ethics in Washington (Plaintiff) v. Executive Office of the President, et al.* Retrieved 28 March 2007 from http://citizensforethics.org/files/Document%2018%20 (11-12-07).pdf