Frontiers in Recordkeeping: Internet Service Providers

Mark Brogan

Mark Brogan is a lecturer in Recordkeeping and Internet studies at Edith Cowan University. He has published on the microeconomics and technology of recordkeeping and has also been involved in the development of multimedia courseware for graduate studies in recordkeeping. Before becoming an academic, Mark spent ten years as a practising archivist and records manager in a variety of positions in university, national and state archives.

This article reports outcomes from research into the Australian Internet Service Provider (ISP) industry. ISPs provide Internet connectivity services to business, government and consumers. Information systems operated by ISPs predominantly serve business purposes, but contain significant depositories of personal and other information. Survey data gathered as a consequence of this research describes divergent data management practice between firms, an outcome attributable in part to the unregulated nature of 'recordkeeping' in this industry.[1] *The author argues that regulatory failure and technology push are combining to create social vulnerability to Internet Service Providers, a situation requiring a proactive role on the part of recordkeeping professionals.*

The Internet industry

From its birth in 1983, the Internet has grown to become the largest computer network in the world. The rate of Internet expansion is quite breathtaking. In *The Emerging Digital Economy,* the United States Department of Commerce reports:

> Fewer than 40 million people around the world were connected to the Internet during 1996. By the end of 1997, more than 100 million people were using the Internet.[2]

According to the Australian Bureau of Statistics, in February 1999, there were nearly 1.3 million Australian households (18% of all households) with access to the Internet, an increase of 50% (423,000) over February 1998.[3] The Bureau further estimated that almost 5 million adults (37% of Australia's total adult

population) accessed the Internet in the 12 months to February 1999 compared to 3 million (23% of all adults) in the previous 12 months.[4]

This spectacular growth in connectivity suggests the pervasiveness of computer networks – so much so that some writers now consider that we are living in a 'digital' or 'cyber' society.[5] The cybersociety does not consist of citizens, but 'netizens', a redefining of the idea of citizenship around connectivity and the Internet. In the rapidly maturing cybersociety, the Internet represents a radical new kind of public space.

Computer networks are also increasing in importance as an enabling technology for economic globalisation. In the operation of financial markets and the daily activities of transnational corporations, computer networks have become indispensable. As the problems for nation states caused by economic globalisation grow, computer networks and the information industries they have spawned also become part of the solution. Advanced technology nations and emerging technology nations all share a common goal – to reshape their economies around information and knowledge industries.

Australia is part of this global race. Our push to become an information economy is supported by a plethora of policy originating and coordinating agencies. At Federal level, these agencies include the National Office of the Information Economy (NOIE), the Department of Industry, Science and Tourism (DIST), the Ministerial Council for the Information Economy, the Department of Foreign Affairs and Trade (DFAT), and the Department of Communications, Information Technology and the Arts, to name but a few. In 1997, a major report entitled *Putting Australia on the New Silk Road: The Role of Trade Policy in Advancing Electronic Commerce* paved the way for national goal setting for the information economy.[6] In December 1998, NOIE released its *Strategic Framework for the Information Economy.*[7]

Internet electronic business (e-business) is categorisable into Business to Business (B2B) and Business to Consumer (B2C) transactions. In March 2000, financial consultants JB Were and Son released *Research Report on the Internet and E-business in Australia,* valuing the Australian B2C market currently at $300 million with growth to $13.1 billion by 2004, a five-year compound growth rate of 113%. The report forecasts global growth in e-business revenues at a compound annual growth rate of 81% over the next five years, from an estimated US$96 billion in 1999, to more than $US1.8 trillion in 2004.[8]

The role of regulation

The rise of the information economy as a public policy issue and the phenomenal expansion of the Internet have resulted in an unprecedented

degree of interest in the need for regulating various kinds of online activity. The breadth of regulatory issues presented by the new technology is truly staggering – digital authentication, encryption, intellectual property, privacy, data protection, cyberspace criminality, equity, freedom of expression, consumer advocacy and complaint resolution. This list does not claim to be exhaustive.

The industry reaction to regulatory possibilities has been mostly negative. In common with their counterparts in the United States, Australian Internet Service Providers have mostly resisted regulation, emphasising its potential to impede the growth of e-business and to retard technological innovation.

On the whole, government has complied with the industry view that it should keep its hands off the industry, conceding not only the possible stultifying effects of regulation, but also its possible impracticality.[9] Instead, it has pursued a policy of industry self-regulation. Under self-regulatory principles, an industry accepts responsibility for the development and policing of a code of practice controlling the activities of firms in the industry. Usually, the code development and compliance monitoring role is performed by the relevant industry association, in this case the Internet Industry Association of Australia (IIA). In February 1999, IIA published an adoption version of its *Internet Industry Code*.[10] The code currently encompasses data privacy, content control and consumer complaint resolution.

In late 1999, in a controversial and notable departure from the self-regulatory model, the Australian Government moved to implement a co-regulatory regime for content control. The *Broadcasting Services Amendment (Online Services) Act 1999* commenced operation on 1 January, 2000.[11] The Act provides for an industry code regulating prohibited content and the issuing of take down notices for materials refused classification under existing censorship guidelines.[12]

Enactment of online content blocking legislation was opposed by a coalition of Internet Service Providers and community groups, including Electronic Frontiers Australia[13] and the Australian Consumers' Association,[14] both long-time community advocates in the cyberspace debate. The debate over content control is symptomatic of the growing public controversy surrounding all forms of net regulation. The policy community for this debate includes telecommunications carriers, Internet Service Providers, professional and industry associations,[15] business, government and a variety of community groups functioning as netizen advocates for the protection of personal data, resolution of complaints against service providers, as well as the more familiar issue of content control.

To date public policy development for the cybersociety has mostly failed to deal with the rights of netizens in any kind of systematic way. Policy development has been piecemeal, dealing with freedom of expression in a de facto way through the development of policy imposing forms of online censorship and, more recently, the right to some form of data privacy.[16]

An important omission concerns data management policy and procedure in ISPs. The remainder of this paper describes the research design and outcomes of a study of Internet Service Provider data management activity undertaken by the author in 1998. The paper concludes with an examination of the concept of recordkeeping in the emerging cybersociety.

Recordkeeping in cyberspace

Of the 5 million Australian users, few possess expert knowledge of the kinds of records created by ISPs. Typically, an Internet Service Provider maintains the following *minimum* business data about clients:

- account details: user ids and passwords, billing and payment data;
- client service agreements: in effect a contract between the subscriber and the ISP describing the terms under which connectivity services are provided; and
- server log information describing use of ISP services by subscribers and others (eg non-domain users visiting sites hosted by the ISP).

Client documents in the form of email, web pages, download and upload documents may also reside on servers.[17]

Server logs

The Internet is a client server technology. As users send requests and receive information, records of this activity are created on servers operated by ISPs and other content publishers such as universities, government agencies and businesses. Minimally, web server transfer logs contain:[18]

- the unique Internet Protocol (IP) address or domain name of the system making the request to the web host;
- the time of the download;
- user's name (if known by user authentication or obtained by the identd[19] protocol);
- the URL requested (including the values of any variables from a form submitted using the GET method);

- the status of the request; and
- the size of the data transmitted.

This data is both private and commercially significant. The commercial significance of the data concerns profiling of subscriber tastes and preferences in terms of sites visited and related download behaviour. An individual's profile information can be linked to an email address, providing telemarketers with sufficient information to construct and implement targeted online marketing campaigns. In its crudest form, telemarketing is familiar to most net users as 'spamming' – sending of unsolicited email messages to individuals and lists.

Because servers are scattered around the global community of Internet users, transfer logs are dispersed offering a significant degree of protection to users. But as organizations move to proxy server technologies as part of their Internet gateway strategy, this protection is being eroded.

A proxy server enables an organisation or ISP to:

- effect economy in Internet services through the caching of frequently accessed sites external to the organisation's firewall; and
- monitor web site access by individuals in organisations, if there is a resolve to do so.

Proxy server user logs contain a single user log of all external web site access. Stein and Bagwill comment :

> A proxy server will log every access to the outside web made by every member of the organisation and track both the IP number of the host making the request and the requested URL.[20]

Rubin, Geer and Ranum conclude that there are risks to users in the use of proxy server technologies:

> Practically all firewalls log and summarise web accesses made through them, presenting the administrator with histograms and statistics of the most frequently accessed sites. Users behind a firewall should assume that their surfing habits are being *audited*, or at least *recorded*, even if nobody reviews the logs.[21]

User profiling capability can be native to server software or may be implemented using third-party solutions such as Funnel Web Pro.[22]

Data management

As the above survey shows, Internet Service Providers are responsible for significant depositories of personal data. Subscribers are vulnerable to the activities of Internet Service Providers, because:

- data gathered about a subscriber's use of the Internet may be disclosed to third parties or used in a manner for which consent has not been given;
- the confidentiality of information contained in communications cannot always be guaranteed in what is substantially an open communications system;
- network security in ISPs is routinely subject to attack by hackers seeking to access, destroy or change data; and
- disposition arrangements for log information are seldom described in client service agreements and mostly involve no reference to data subjects.

Ideally, ISPs will be accountable to netizens for their management of personal data and this is one of the objectives of the *Internet Industry Code of Practice.* However the code does not deal with recordkeeping in a comprehensive way and adherence to the code is voluntary. Important questions for the industry, public policy makers and netizens concern:

- levels of code compliance within current voluntary arrangements; and
- whether the code requires development to encompass the broad range of recordkeeping issues of potential significance to netizens.

Survey results and interpretation

These questions were addressed in a survey of ISPs undertaken by the author in mid-1998. Although, the survey attempted to measure self-regulatory compliance across a range of issues and not just recordkeeping, it did furnish some interesting insights into data management policy, procedure and practice of interest to the recordkeeping community.

The study faced an initial challenge of constructing a survey method enabling it to work with the estimated six hundred (600) ISPs existing at the time.[23] The first task in research design, therefore, was to identify a smaller sample population suited to the conduct of an unfunded study. To preserve 'generalisability', it was decided to construct a disproportionate purposive sample based on medium to large ISPs, where capitalisation and revenue generation suggested the greatest likelihood of self-regulatory compliance. The total number of data subjects in the smaller population was thirty, including:

- some of Australia's largest ISP operators measured in terms of the subscriber base;[24]

- a smaller number of medium-sized operators consisting of ISPs with more than one thousand subscribers; and
- a much smaller number of operators with a subscriber base consisting of less than five hundred users.

The sample population included both commercial and educational providers. Acknowledged limitations of the study arise from:

- the commercially sensitive nature of the information requested (this is important both in terms of the response rate and the reliability of information provided as ISPs are reluctant to reveal information as basic as the number of subscribers on their books); and
- the complexity of some dimensions (data protection is an obvious example of a dimension justifying investigation in its own right).

The purposive nature of the sample suggests greater reliability than would normally be found with a small sample population and the response rate recorded (33%). Findings of this regulatory study with recordkeeping significance concern code subscription, log management and management of the access regime.

Code subscription

In terms of formal adoption, the survey data revealed a very low level of Internet Industry Association (IIA) support for the draft code of practice amongst respondents (25%). Because of the small sample size, and its disproportionate character, this outcome was not considered reliable and generalisable to the whole population.[25] To provide a more reliable measure, the IIA list of members published on Internet[26] was compared with the May 1998 edition of the authoritative Cynosure listing of Australian Internet Service Providers.[27] This method produced a measure of 5.3% of all Internet Access Providers: that is, a result even lower than the sample population measure of formal adoption.

The result is significant for recordkeepers because it suggests very low levels of industry support for the warrant contained in current industry code. This warrant is incidental in its treatment of recordkeeping, but does:

- commit code subscribers to uphold the Federal Government's *National Principles for the Fair Handling of Private Information;*[28] and
- commit code subscribers to the erasure of information collected about users which is no longer accurate or no longer required or requested to be removed by the user.[29]

Log management

Two kinds of logs are kept by ISPs: transfer logs[30] describing download activity and subscriber login files describing user login details. The survey revealed little uniformity in retention policy and practice for log information.

Transfer logs

Three respondents indicated that they retained proxy server transfer logs. The retention period ranged from one month to indefinitely. In interview, an ISP where logs are retained indefinitely considered that this was an exercise in risk management. The systems operator commented that 'if it becomes necessary to show where people are going, then we can'. A major industry player where access logs are retained for seven years viewed this as a requirement under taxation law. Another respondent considered that no business case could be made for retaining log information, and practice at this ISP involved rolling the information over in accordance with the availability of off-line storage.

Subscriber login files

Because of file size, most ISPs do not retain web server access logs. The retention of subscriber login files which minimally record the time, date and duration of subscriber online sessions is more commonplace. Of the seven respondents who answered this question, all indicated that they retained subscriber login files. Once again, there was little uniformity in the retention period with an effective range of one month to seven years recorded.

The question of log retention is extremely significant. Taken together, proxy server transfer logs and subscriber login files enable the reconstruction of a subscriber's use history inclusive of the dates and times of sessions, sites visited and files downloaded. In the one ISP where archiving of access logs has been systematically implemented from its inception, a systems operator commented that it would be technically possible to reconstruct a user's use history covering some four years of ISP operations. Clearly, subscribers have an interest in disposal practice for log files created by their service provider. But research conducted into disclosure revealed that only 17% of survey ISPs disclosed data management practice in their client service agreement.

Access

In addition to a well-defined policy, best practice principles in the management of subscriber information suggest that ISPs should have written procedures for the handling of requests for private information by third parties. Of respondents, three representing 38% of respondents claimed to have written

procedures. However, the incidence of third-party requests was very high, with six respondents representing 75% of respondents reporting that they had received at least one such third-party request.

Analysis of event histories showed that requests from law enforcement agencies comprise the most common form of third-party request, with 83% of respondents recording at least one request from this source. Reliable data on the number of third-party requests received by ISPs was difficult to obtain, with many respondents either not quantifying requests or preferring a narrative answer (eg 'a few' or 'numerous'). In addition to law enforcement agencies, the largest ISP respondent had received requests for subscriber information from the Telecommunications Ombudsman and law firms.

Analysis

In summary, the study revealed:

- low levels of compliance with the IIA Code of Conduct measured in terms of code subscription; and
- significant variation in data management practice in the respondent sample. This variation encompasses creation and disposal of server access and login files. Dependent variables include concepts of warrant as perceived by systems operators, client group and technology in use.

Although these findings must be treated with caution because of the small sample size, they are significant. Variation of policy and procedure are suggestive on the one hand of an immature industry, and on the other, an industry where the warrant for recordkeeping is basically unclear to participating firms.

This begs the question of what role (if any) recordkeeping professionals should play in the development of public policy on recordkeeping in ISPs.

Perspectives on recordkeeping

Clearly, inconsistent data management in ISPs might be thought of as describing a recordkeeping problem of significance to both the industry and society at large. But recordkeeping professionals have little to contribute to the efficient operation of ISPs in terms of day-to-day data management, an activity which is regarded as the preserve of systems operators and other information technology professionals.

The real scope for involvement concerns the social and political dimensions of recordkeeping, where it can be argued that involvement of recordkeeping

advocates is long overdue. Specifically, the industry requires the involvement of recordkeeping professionals to assist it to solve the following basic problems now affecting this industry:

- what kinds of disposal and access regimes should exist for private data created as a consequence of ISP activity? and
- what kind of warrant for recordkeeping can or should exist for the Internet Service Provider industry?

Access and disposal: social and political dimensions

In a recent interview, Phil Zimmermann, the architect of the World Wide Web consortium's PGP privacy specification was asked what new possibilities for surveillance might emerge around computer networks and most particularly the Internet. He replied:

> ...scanning for subversive words in all of your email – and I mean *all* of your email, surveillance cameras that can recognize human faces and match them against drivers' licence databases. You could even have cameras on the streets that can recognize everyone walking down the street. As Moore's Law makes things faster and faster, the capabilities become even greater.
>
> You could track people's movements. You could ask an expert system to give you a list of people who may have done something inappropriate in the past two years.[31]

Zimmermann's comments suggest the increasing vulnerability of society to 'dataveillance', the gathering of intelligence about individuals via computer networks.[32] As proxy server and profiling technology increases in sophistication, so does the appeal of dataveillance. Surveillance activity which once would have been too expensive for organizations and government to undertake, can now proceed in an automated fashion with no or minimal operating cost. Because most Internet users use connectivity services supplied by their employers, increasing levels of dataveillance can be justified in terms of an employer's right to ensure that business systems are being used for business purposes. Anecdotal evidence gathered as part of the study suggested that some ISPs have identified dataveillance performed on behalf of client organizations as an important new value-added service opportunity.

At the very heart of this vulnerability is the way in which Internet Service Providers manage access to and disposal of personal data. This study shows no embedded concept of industry best practice. This is not an unexpected result given the unsatisfactory prescription contained within the current voluntary code. Sections 9 (c) and (d) of the code which deal with expungement and ultimate disposal are problematic because:

- they are insufficiently explicit about classes of data and their retention periods;
- transfer and subscriber login files can have a legal or evidential value; and
- an Internet Service Provider may be required to establish due diligence in the operation of its services through reference to log information.

Case history is in its infancy, but logs have been used as evidence against individuals who misuse connectivity services. In case law today, 'misuse' typically involves the downloading of violent or 'objectionable' materials which would otherwise be refused public access classification, or the use of a service to hack another computer system.

Taken with other information, log data may also be important in establishing proof of transactions where one or more parties repudiate the transaction. Logs also provide a kind of proof of online publication, which may be important in disputes over intellectual property. In other cases involving alleged breach of copyright contained in online materials, logs provide evidence of when a download takes place, the IP address of the machine concerned and the nature of the files downloaded. It is unlikely that the simple prescription contained in the current code will serve the industry well.

To be weighed against the many valid purposes to which log data may be put is the potential nightmare of the surveillance society described by Zimmermann. Clearly current settings are manifestly inappropriate, if, as one survey respondent suggested, managing risk appropriately involves the archiving of logs so that 'if it becomes necessary to show where people are going, then we can'.

Conclusion: a warrant for recordkeeping?

From this research, it is plain that data management policy and practice in Internet Service Providers has legal, social and political dimensions which warrant its consideration as recordkeeping activity. The research has also shown that within a small purposive sample of firms, recordkeeping responsibilities are interpreted in different ways. Such an outcome is consistent with the fact that society is yet to determine what warrant, if any, should exist for recordkeeping in this industry.

Recordkeeping professionals have an obvious role to play in assisting the industry and community to develop a better understanding of the kind of warrant which should exist, and to develop a notion of best practice which can be applied across the industry. In engaging the community, government,

the industry, the professions and other interested groups, they will employ their discipline-based knowledge of appraisal, disposal and the management of an access regime.

But life at recordkeeping's frontier will not be easy. Because of rapid technological change, the ground will be constantly shifting. In a changing technology environment, recordkeeping professionals will need to grapple with complex and important issues concerning:

- the circumstances under which records created by connectivity service providers might be deemed reliable – for example, although they are finding increasing use in dataveillance, the reliability of server log information is currently questionable;
- the nature of 'cyber-rights' and their implications in terms of recordkeeping practice;
- the nature of risk to individuals and whole communities posed by various kinds of recordkeeping policy and practice; and
- the nature and effectiveness of regulatory regimes for ensuring industry compliance with recordkeeping standards.

At the frontier, recordkeeping professionals will need to reconcile the apparently conflicting demands of cyber-rights advocates, governments and industry. The ethical dimensions of recordkeeping policy and practice will need to be foremost in their minds and their instinct for ensuring evidence may at times necessarily take a back seat. In particular, the potential for increasing levels of dataveillance facilitated by passive data gathering and retention cannot be ignored.

If they rise to the challenges of recordkeeping in a cybersociety, archivists and records managers will be taken more seriously by government and society. They may find that in common with Phil Zimmermann, they too 'have a reason to get up on Monday morning'.[33]

ENDNOTES

1 According to the Australian Standard: Records Management Part I (AS 4390.1) the term 'recordkeeping', refers to the 'making and maintaining of complete, accurate and reliable evidence of business transactions in the form of recorded information'. The systems investigated in this research mostly do not meet the requirements for recordkeeping systems as defined by AS 4390, but function as repositories for records which describe business transactions, ie transactions between user and various providers of Internet services.

2 United States Government, Department of Commerce, Secretariat on Electronic Commerce, *The Emerging Digital Economy*, June 1998, at *www.ecommerce.gov/ederept.pdf*.

3 Gordon Finlayson, *Australian Internet Usage Reaches Five Million,* at *www.zdnet.com.au/zdnn/stories/zdnn_display/au0000347.html* (March 2000).

4 *Ibid.*

5 Early commentators on the social impact of computer networks such as Arturo Escobar and Steven Jones popularised terms such as 'cybersociety' and 'cyberculture'. For an explanation of these terms see:

Arturo Escobar, 'Welcome to Cyberia: Notes on the Anthropology of Cyberculture', *Current Anthropology*, vol. 35, no. 3, 1994, pp. 211–31; and

Steven G Jones, 'Understanding Community in the Information Age', *Cybersociety*, Sage Publications Inc., Thousand Oaks, 1995, pp. 11–32.

6 Commonwealth of Australia, Department of Foreign Affairs and Trade, *Putting Australia on the Silk Road: The Role of Trade Policy in Advancing Electronic Commerce*, 1997, summary at *www.dfat.gov.au/nsr/silk_exec.html* (April 2000).

7 Commonwealth of Australia, Department for Communications, Information Technology and the Arts, *A Strategic Framework for the Information Economy: Identifying Priorities for Action*, 1998, at *www.noie.gov.au/docs/strategy/strategicframework.html* (February 1999).

8 JB Were & Son, *Research Report: The Internet and E-Business in Australia,* March 2000, p. 4.

9 The global nature of the Internet and technology factors emphasise the limitations of classic regulatory approaches. For a discussion of these factors see David R Johnson and David G Post, *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law*, 1996, at *www.cli.org/emdraft.html.*

10 See Internet Industry Association, *Internet Industry Code of Practice*, Version 4.2, 1999, at *www.iia.net.au/Code4_2.doc.*

11 Commonwealth of Australia, *Broadcasting Services Amendment (Online Services) Act 1999*, at *scaleplus.law.gov.au/html/comact/10/6005/top.htm* (March 2000).

12 For a concise summary of the Act see Alphalink's web page located at *www.alphalink.com.au/bsaosa.htm* (March 2000).

13 EFA describes itself as 'a non-profit national organisation formed to protect and promote the civil liberties of users and operators of computer based communications systems'. EFA's home page is at *www.efa.org.au/Welcome.html.*

14 See Australian Consumers' Association home page at *203.108.76.38/default.asp.*

15 For example, the Australian Computer Society (ACS) and the Internet Industry Association.

16 In late 1998, the Commonwealth government announced its intention to pursue data privacy law, see Carlina Tan-Van Baren, 'Federal Move for National Privacy Laws', *The West Australian*, Thursday 17 December 1998, p. 41.

17 Beginning with David Bearman's classic essay, recordkeeping issues with electronic mail have been the subject of considerable publication activity and are not the focus of this study. See D Bearman, 'Archival Methods', *Archives and Informatics*, vol. 3, no. 1, 1989.

18 Lincoln D. Stein and Bob Bagwill, *World Wide Web Security FAQ,* at *css.tuu.utas.edu.au/~brong/mirror/websecure/wwwsf6.html#*Q51 (June 1998).

19 Identd = Identity, referring to a Unix program enabling discovery of the identity of a user.

20 World Wide Web Consortium (W3C), *World Wide Web Security FAQ: 8. Server Logs and Privacy*, at *www.w3.org/Security/Faq/wwwsf6.html* (March 2000).

21 *Ibid.*

22 For a short review of Funnel Web Pro functionality, see James Riley, 'Funnel Web Pro Stalks ISP Market', *The Australian: Computers and High Technology*, Tuesday 17 March 1998, p. 8.

23 Figure based on the authoritative Cynosure list online at *www.cynosure.com.au/isp/* published monthly by *Internet.au: Australia's complete guide to the Internet.*

24 The largest participating ISP claimed in its participant profile to have 200,000 subscribers and to employ 510 full-time staff.

25 Seen as favouring *over*-representation of member providers.

26 Available at *www.iia.asn.au/iia_mem_list.htm.*

27 Available at *www.cynosure.com.au/isp/* published monthly by *Internet.au: Australia's complete guide to the Internet.*

28 See Office of the Privacy Commissioner, *National Principles for the Fair Handling of Private Information*, revised ed., 1999, at *www.privacy.gov.au/publications/index.html.* Section 4.2 of the *Principles* declares that 'an organisation should take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose'.

29 Internet Industry Association, *Internet Industry Code of Practice*, section 9.3 (c) and (d).

30 Also referred to as access logs.

31 Ian Grayson, 'The World According to Phil Zimmermann', *The Australian: Computers/ News Features*, Tuesday 9 February 1999, p. 57.

32 Dataveillance = the systematic monitoring of people's actions or communications through the application of information technology. See Roger Clarke, *Information Technology and Dataveillance*, 1998, at *www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html.*

33 Grayson, p. 57.