TOWARDS ELECTRONIC DEMOCRACY: THE IMPACT OF TECHNOLOGICAL CHANGE ON THE OFFICIAL INFORMATION ACT 1982

Jessica White*

The paper considers the impact of recent technological advancements on the law and policy of the Official Information Act 1982. As the capacity and potential of technology increases, the ability to store, retrieve, and disseminate information could add immense value to the purposes and operation of the Act. However, there are two substantial difficulties with the technological changes. First, there are insufficient efforts to improve access to technology for certain segments of society. Second, co-ordination between initiatives to improve government information management systems have so far proved ineffective. These two problems pose substantial threats to the usefulness of the new technology. Consequently, the paper concludes by recommending that a co-ordinated, educational approach led by central government will ensure that the Act's benefits for citizens are enhanced by technological change, rather than undermined by it.

I INTRODUCTION

"Knowledge will forever govern ignorance: and a people who mean to be their own governours, must arm themselves with the power knowledge gives."[1] A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy or perhaps both.

New Zealand in 1982 was a world that would seem foreign and cumbersome to those of us living in the twenty-first century. No typical business had a computer in every office, nor was it expected that such a thing would ever be feasible. Certainly having a computer at home was almost unheard of. Where there were computers, there was no internet and no email.

---

* This article is an edited version of a paper submitted in fulfilment of the requirements of the LLB(Hons) degree at Victoria University of Wellington, 2002.

1 Interview with James Madison, President of the United States 1809-1817 (M T Barry, 4 August 1822), cited in On These Walls: Inscriptions and Quotations in the Buildings of the Library of Congress <http://lcweb.loc.gov/loc/walls/madison.html> (last accessed 4 March 2003).

2003 marks the twenty-first anniversary of the passing of the Official Information Act 1982 ("the Act").[2] To say that technological advances in those 21 years have transformed the vast majority of work places, and life at home, is no overstatement. Living without computers would now seriously impede our ability to gather information, conduct business and form personal relationships. Yet this is the environment in which one of our most significant constitutional pieces of legislation was passed.

This article assesses the impact of the new technological environment on the law and policy of the Act. It explores potential advantages and disadvantages of the new environment, and evaluates initiatives currently in place to recognise the presence of electronic information in organisations in the scope of the Act. Finally, it assesses whether changes to legislation or behaviour are necessary to ensure the Act still fulfils its objectives today.

II BACKGROUND AND LEGISLATIVE HISTORY

Before investigating the effect of the modern environment on official information, it is necessary to have an understanding of the events leading to the introduction of the Act, and its purpose.

Until 1982, the release of official information had been governed by the Official Secrets Act 1951. Under that Act, the presumption was that information should not be disclosed unless there was good reason to do so.[3] The key provision made it illegal for a government officer to communicate official information to any person other than a person to whom he or she was authorised to communicate it, or a person to whom it was in the interests of the State to communicate it.[4] Much of the information that was disclosed was done so more or less at the discretion of the individual government departments and their officers, and what they considered they were authorised to reveal.

The New Zealand Committee on Official Information ("the Danks Committee") conducted a review in 1980. The Committee was established after a chain of events triggered by the then Chief

---

2 Many other countries around the world have also adopted freedom of information legislation. Examples include the United States' Freedom of Information Act 1966, Australia's Freedom of Information Act 1982 (Cth), Canada's Access to Information Act 1983 and more recently the United Kingdom's Freedom of Information Act 2000. The trend toward legislation of this nature seems set to continue: David Banisar Freedom of Information and Access to Government Records Around the World <http://www.freedominfo.org/survey/> (last accessed 5 January 2003).

3 Official Secrets Act 1951, s 6.

4 Official Secrets Act 1951, s 6.

Ombudsman, Sir Guy Powles, who had difficulty trying to obtain information for a review on the New Zealand Security Intelligence Service.[5] Their conclusion was that:[6]

> … it is no longer acceptable to set out a sweeping rationale for the protection of official information or to expect that the public will accept in the future that certain areas of government business are inviolate simply because the government says so.

The Committee concluded that legislation should be introduced to change the presumption to one of openness. The rationale was expressed on the following bases:[7]

- *Participation*: members of the public can better perform their roles in a democracy if they are better informed about issues under consideration. The credibility of political decisions is arguably enhanced as a result;
- *Accountability*: those in government, and in the executive, can be held accountable more easily. Their mistakes and errors of judgement cannot be hidden through the unjustified concealment of information;
- *Effective government*: this is achieved by members of the public being able to participate in the process of policy development. Decisions can more easily be understood and accepted; and
- *Concern for individuals*: individuals should be able to access information that the government holds on them, and be able to correct it if necessary.

Lastly, it was acknowledged that the government has a particularly pervasive role in the lives of New Zealanders, giving them an even greater interest in the activities of government.[8] The principles by which the Danks Committee rationalised the introduction of the Act are as relevant in 2003 as they were in 1982.

At the same time, the presumption of openness was just that: a presumption. A blanket policy of openness was not considered appropriate. The Committee set out some compelling reasons to protect some types of information, which are discussed further below.

---

5 Robert Gregory (ed) *The Official Information Act 1982: A Beginning* (New Zealand Institute of Public Administration, Wellington, 1984) 32.

6 New Zealand Committee on Official Information *Towards Open Government* (Government Printer, Wellington, 1980) 20.

7 New Zealand Committee on Official Information, above, 14-16.

8 New Zealand Committee on Official Information, above, 14.

The recommendations of the Danks Committee are reflected in the purpose provision of the Act, section 4:[9]

> 4. Purposes – The purposes of this Act are, consistently with the principle of the Executive Government's responsibility to Parliament, –
>
> (a) To increase progressively the availability of official information to the people of New Zealand in order –
>
> (i) To enable their more effective participation in the making and administration of laws and policies; and
>
> (ii) To promote the accountability of Ministers of the Crown and officials, – and thereby to enhance respect for the law and to promote the good government of New Zealand:
>
> (b) To provide for proper access by each person to official information relating to that person:
>
> (c) To protect official information to the extent consistent with the public interest and the preservation of personal privacy.

At the heart of the Act is the principle of availability set out in section 5. The presumption is that information shall be made available unless there is good reason for withholding it.[10] New Zealand's legislation is unique in that it does not refer to 'documents' or 'records', but 'information'. This term is not defined in the Act. McMullin J in *Commissioner of Police v Ombudsman*[11] decided that the drafters must have intended it to have its ordinary definition – that which informs, instructs, tells or makes aware.[12] Electronic information clearly falls within the scope of the Act under this approach. As Cooke P pointed out in the same case, the Act can be described as a constitutional piece of legislation and has permeating importance;[13] the nature of it means the spirit of the Act should be given effect to.[14] Evidently, the placing of electronic information beyond the scope of the Act would not be in keeping with its spirit. Notwithstanding this view, some District Court cases have discussed whether official information legislation applies to information which is not recorded in writing. The Court in those instances decided that it did not.[15] However, the Ombudsman's view is

---

9 Official Information Act 1982, s 4.

10 Official Information Act 1982, s 5.

11 *Commissioner of Police v Ombudsman* [1988] 1 NZLR 385 (CA).

12 *Commissioner of Police v Ombudsman*, above, 402, McMullin J.

13 *Commissioner of Police v Ombudsman*, above, 391, Cooke P.

14 *Commissioner of Police v Ombudsman*, above, 398, Cooke P.

15 See *Ross v Tamaki City Council* [1990] DCR 11 and *Aldous v Auckland City Council* [1990] DCR 385.

that non-documentary information is in fact included.[16] Furthermore, as Jeffries J said in the High Court in *Commissioner of Police*:[17]

> Perhaps the most outstanding feature of the definition is that the word "information" is used, which dramatically broadens the scope of the whole Act. The stuff of what is held by Departments, Ministers, or organisations is not confined to the written word but embraces any knowledge, however gained or held, by the named bodies in their official capacities.

The Court of Appeal did not disagree with this. Given the approach of the High Court and the Ombudsman, then, it seems beyond dispute that electronic information falls within the definition of information. The purpose and policy behind the Act demand that such an approach be taken. The Cabinet Manual supports this view, saying, "[t]he definition of information is not confined only to information on paper. Official information can include sound recordings, film, computer records, emails and knowledge carried in someone's head".[18] Therefore, given technological developments since its enactment, there is more information within the scope of the Act, and information is more accessible.

The term 'document' is defined in the Act (for the purposes of sections 16 and 17, which deal with information held in a document) and is defined broadly and inclusively.[19] For example, it includes cassette tapes, the negatives of photographs, and maps. Certainly, documents may include electronic documents.

Sir Kenneth Keith drew an important distinction between New Zealand's freedom of information legislation and that of other countries. Under the New Zealand Act, it is not the type of document requested that determines whether it may be revealed, but rather the substance of it (for example, national security) or the process by which it arose (for example, information passed to the New Zealand government in confidence from another government).[20] No distinction is made between the various forms of information in the statute. This means the fact that information is stored electronically does not in itself determine whether it may be withheld.

Several sections outline reasons that may justify the withholding of information. These broadly cover the same substantive areas as the Danks Committee suggested. Section 6 lists conclusive

---

16 Sir Brian Elwood and Judge Anand Satyanand "Application of Official Information Legislation to Non-documentary Information" (1998) 4 Ombudsmen Quarterly Review 1.

17 *Commissioner of Police v Ombudsman* [1985] 1 NZLR 578, 586 (HC).

18 Cabinet Office "Chapter 6, Official Information: Protection, Availability and Disclosure" in *Cabinet Manual* <http://www.dpmc.govt.nz/cabinet/manual/6.html> para 6.23 (last accessed 5 January 2003).

19 Official Information Act 1982, s 2.

20 Sir Kenneth Keith "The Official Information Act 1982" in Robert Gregory (ed) *The Official Information Act: A Beginning* (New Zealand Institute of Public Administration, Wellington, 1984) 36.

reasons why information can be withheld. These include information relating to matters of security or defence, maintenance of the law, the safety of any person, the economy, or matters referred in confidence to the New Zealand government by other governments or international organisations. Other reasons overcoming the section 5 presumption of availability are contained in section 9. These include withholding information to protect individual privacy, releasing the information to prevent unreasonable prejudice to someone's commercial position, or to maintain constitutional conventions. Finally, section 18 provides several administrative-type grounds for refusing a request for information.[21]

Nowhere in the Act, nor in the Danks Committee report, is any kind of technological change affecting official information directly contemplated. It is possible that any envisaged technological change would not change the nature of information recorded, and therefore no special provision was necessary. One thing that is clear, however, is that:[22]

> Departmental chief executives and managers of agencies in the wider state sector (where those agencies are subject to the Act) are responsible for ensuring compliance with the Act within their organisations, and must actively ensure that adequate systems, information and training are available to relevant staff.

This implies that the relevant systems must reflect changing environments. This leads us to consider how these changes have manifested in recent times.

III STRENGTHS OF THE ACT IN TIMES OF ADVANCING TECHNOLOGY

Many would argue that advancements in computer technology have changed the face of information across society. Its physical nature is different. It can be stored in a number of locations. It is more portable than a stack of heavy papers, if use is made of a floppy disk or compact disk. Large volumes of information can be handled quickly and easily. Filtering capabilities of modern computers mean that relevant, specific information is easier to find and collate. Overall, ease of access is increased. This means the public is more likely to gain access to and use information, which in turn could potentially lead to a more effective democracy. Even in the absence of electronic information, more active and effective participation by the public was envisaged as more likely under the Act, and considered vital to the interests of New Zealand as a democracy by the Danks Committee.[23] Evidently there is potential for the electronic environment to enhance participation.

---

21 Official Information Act 1982, s 18. Examples include where information is or soon will be made publicly available (s 18(d)), or where the request is frivolous or vexatious (s 18(h)).

22 Cabinet Office "Chapter 6, Official Information: Protection, Availability and Disclosure" in *Cabinet Manual* <http://www.dpmc.govt.nz/cabinet/manual/6.html> para 6.13 (last accessed 5 January 2003).

23 New Zealand Committee on Official Information *Towards Open Government* (Government Printer, Wellington, 1980) 14.

In 1995, the Australian Law Reform Commission conducted a review of the federal Freedom of Information Act 1982.[24] They found that technological advances are generally enhancing the ways in which the government provides information. More information is being made available on the internet, and having the information available in that way makes it accessible to a wider audience.[25] The New Zealand government website is a starting point for such availability in New Zealand.[26] This may reduce transaction and administration costs, due to the decline in the amount of direct correspondence between the organisation and members of the public. However, there is a question over whether access to media like the internet are as widespread as they should be for this to really take effect. This is discussed further below.

It is also true that only official information "held" by a particular government department or organisation is subject to the Act.[27] In the Australian Law Reform Commission's review, it was suggested that documents are "in the possession of"[28] (the equivalent to "held" in our legislation) an agency where the information is accessible through electronic networks such as the internet. The Commission rejected this idea, saying that information is not in the possession of an agency merely because the agency could get access to that information through a computer system or network.[29] This approach would probably be taken in New Zealand as well, given the broad similarities in the law and the environment, to mean that only downloaded information is considered to be actually held by the organisation.

The approach taken in privacy law may be instructive. Agencies that hold personal information in such a way that it can readily be retrieved are under certain obligations under the Privacy Act 1993.[30] The approach to "held" under this legislation was discussed in *Mitchell v Police Commissioner*;[31] it was said that simply because personal information might not be in the agency's actual physical custody at the time a request is made, does not mean it is not held by the agency.

---

24 Australian Law Reform Commission *Open Government: A Review of the Federal Freedom of Information Act 1982* <http://www.austlii.edu.au/au/other/alrc/publications/reports/77/ALRC77.html> (last accessed 5 January 2003).

25 Australian Law Reform Commission, above, para 2.6.

26 New Zealand Government portal <http://www.govt.nz> (last accessed 5 January 2003).

27 Official Information Act 1982, s 2.

28 Freedom of Information Act 1982 (Cth), ss 4 and 15.

29 Australian Law Reform Commission *Open Government: A Review of the Federal Freedom of Information Act 1982* <http://www.austlii.edu.au/au/other/alrc/publications/reports/77/ALRC77.html> (last accessed 5 January 2003) para 7.4. New Zealand Law Commission *Review of the Official Information Act 1982* <http://www.lawcom.govt.nz> NZLC R40 did not mention the potential use of the internet as broadening the scope of government-held information in this way.

30 Privacy Act 1993, s 6, Principle 6: Access to Personal Information.

31 *Mitchell v Police Commissioner* [1995] NZAR 274 (Complaints Review Tribunal).

The concept of "holding" should be given a wide meaning to include all cases where the agency has control over the information.[32] It was also said that despite the police officer involved not knowing where the information was, the information was still retrievable.[33] This broad interpretation also sits well with the language of the Act.

Aside from the above, there are the significant time and cost savings that the use of electronic media can bring about. Requests for official information can even be circumvented altogether if the information is made publicly available.[34] The potential for this expands through the use of the internet. This kind of approach would be entirely consistent with the purposes of the Act, especially section 4(a): "To increase progressively the availability of official information to the people of New Zealand …".

The time limit for dealing with requests is 20 working days,[35] but there is scope for this to shorten, or at least for pressure on people dealing with requests to ease. The Law Commission noted this when they conducted their review of the Act in 1997.[36] They considered that the Act implicitly advocates the progressive release of official information to the public without it being requested. They also indicated that they thought it appropriate for the State Services Commission to monitor the progress of agencies within the scope of the Act in terms of their information technology implementation and overall information management, with a view to assessing whether it was appropriate to reduce the time limit. More specifically, the Commission recommended that the government review the 20-working days limit under section 15(1) in three years' time (in the year 2000) and consider reducing it to 15 days. Such a reduction would recognise the faster retrieval times that are possible due to electronic information storage.[37] Amendments to the law have yet to be made.

In the above respects, it appears the Act is equipped to deal with modern technology despite the fact that it was drafted without the detailed knowledge of the potential development in that area. The advantages that information technology can bring to requests for official information can be summed up as follows:[38]

---

32 *Mitchell v Police Commissioner*, above, 285-286.

33 *Mitchell v Police Commissioner*, above, 286.

34 Official Information Act 1982, s 18(a).

35 Official Information Act 1982, s 15(1).

36 New Zealand Law Commission *Review of the Official Information Act 1982* at <http://www.lawcom.govt.nz> NZLC R 40 (last accessed 5 January 2003).

37 New Zealand Law Commission, above, para 173.

38 Ted Sieper "Pricing–Costing and Pricing of Government Information. What Are the Issues?" in *Governance in Cyberspace Series: Digital Technology and Development of Government Policy* <http://www.naturespace.co.nz/ed/archive/trespric.htm> (last accessed 5 January 2003).

> In this context, the significance of electronic dissemination is found in the more useful forms in which traditional types of government held information can be provided, the reduction in the cost of provision, the many new ways in which such information can act as an input into further value added products, and the increasing scope for users themselves to transform and work with such information.

IV PROBLEMS THAT THE NEW ENVIRONMENT MAY PRESENT

Information technology, while it improves access to official information, is not without its difficulties. The storage of information in an electronic form has different challenges to storage of information on paper. These challenges are investigated in this section.

It is important to remember that while general security of information is not directly dealt with by the Act, section 4(c) specifically states that one of the purposes of the Act is to protect official information to the extent consistent with public interest and the protection of personal privacy. The Government Communications Security Bureau (GCSB) has looked comprehensively at the potential security problems that computer systems may face in general.[39] Security, or protection of information processed by a computer system, comprises an assessment of three areas:[40]

- *Confidentiality*: information must not be made available or disclosed to unauthorised individuals, entities, or processes;
- *Integrity:* data must not be altered or destroyed in an unauthorised manner, and accuracy and consistency must be preserved regardless of changes; and
- *Availability*: information must be accessible and useable on demand by authorised entities.

The GCSB acknowledges that while computer systems have provided organisations with highly efficient and accessible data storage and processing facilities, they have also exposed the organisations with those systems to a new set of risks and threats.[41] According to the GCSB, there are four aspects of modern computer systems that expose them to risk: the density of information, system accessibility, complexity, and electronic vulnerability.[42] Computer systems and communications systems allow the storage and analysis of very large amounts of data and information. This creates the risk of rapid and covert copying to remote locations. Systems are often designed to provide access to the largest possible number of users, and it is possible that some gain access outside of the intended group. Those who do have legitimate access may use it outside of

---

39 Government Communications Security Bureau <http://www.gcsb.govt.nz> (last accessed 5 January 2003).

40 Interdepartmental Committee on Security *Security in the Government Sector* <http://www.security.govt.nz/sigs/index.html> (last accessed 5 January 2003) 1-2.

41 Government Communications Security Bureau "Chapter 1: The Vulnerabilities of Computer Systems" in *New Zealand Security of Information Technology Publication 100: The Security of Computer Systems* <http://www.gcsb.govt.nz/nzsit/100/100chap1.htm> (last accessed 5 January 2003).

42 Government Communications Security Bureau, above, para 103.

physically secure premises. Systems are also complex and have a wide range of components in terms of hardware, software, and the types of functions they allow people to perform. Finally, systems are also vulnerable to electronic attacks due to the technology used to process and store information.[43]

Electronic information is often duplicated – this can happen, for example, when backups are made, or when information is shared across an organisation or between organisations. Wherever there is duplication, data integrity is immediately an issue. It is possible for several different versions of the same document to exist in an organisation at the same time. Inconsistencies can be significant. From an Official Information Act point of view, a concern arises that the information which may be released is not the official version.

The effect of security measures, or the lack of them, is pervasive and relates to all kinds of information, whether it is on paper, electronic, in a computer memory, on a communication line, computer disk, tape or screen. Arguably, though, the effect of the lack of security on electronic information is greater, because electronic material is subjected to risks of both physical and electronic kinds.

Electronic technology also has the potential to greatly increase the mass of information that is available. This could lead to more official time being devoted to processing requests, and may offset gains made from the reduction in processing times for individual pieces of information due to, for example, faster retrieval times.

Systems that contain electronic and other forms of information are also subject to threat from both inside and outside the organisation. Threats to systems include sabotage, fraud, theft, vandalism, interception of communications lines, electromagnetic radiation, or misuse.[44] If these occur in organisations that are within the scope of the Act, they may jeopardise the availability and quality of information that is available. Without sufficient protection of official information held by such organisations, there can be no confidence that the aims of the Act can be achieved. If electronic information that is released from an unsecured system is relied on by members of the public in making their democratic choices, are we any better off as a country than if the information had never been released at all? Voting in a general election is an example. Basing one's vote on information that is not correct potentially has dramatic ramifications.

It is also worth noting here that organisations within the scope of the Act are under multiple obligations. Section 4 of the Act, which mentions the need to preserve personal privacy,[45] needs to interface in practice with section 6 of the Privacy Act 1993, which outlines information privacy

---

43 Government Communications Security Bureau, above, paras 103-104.

44 Government Communications Security Bureau, above, paras 107-112.

45 Official Information Act 1982, s 4(c).

principles. Four particularly relevant ones are: Principle 5, storage and security of personal information; Principle 6, access to personal information; Principle 8, accuracy of personal information; and Principle 11, disclosure of personal information.[46] It is not only the Official Information Act 1982 that needs to be borne in mind by officials when designing or implementing information systems.

If security measures do not keep pace with advancing technology, members of the public may gain access to material that they were not intended to see, because there is good reason to withhold it under section 5 of the Act. With an increasing amount of government activity, such as policy development, conducted through the use of computer systems, there may be a risk that informal debates, opinions or ideas expressed by people in departments or organisations might accidentally be available. This could be damaging to the policy development process. It is also not consistent with the Act, which clearly recognises that there is a balance between the public interest and the government's need to keep certain things from the public.[47]

Classification systems are another problem created by new technology. Usually if a document is considered to contain information that is sensitive, it is flagged with the appropriate classification. In itself, having a classification does not provide good reason for withholding information under the Act – however, the concern is that classification should be kept consistent across all the mediums it is contained in, for example, if it is held in both a paper form and an electronic form. The problem arises because of version control; it is easier when working in electronic form to create several versions of a document, and then change certain versions and not others.

Another problem is inequality of access amongst members of the public. The usefulness of the internet for commercial and government services has highlighted the importance of ensuring widespread internet access by citizens.[48] Making official information available through new media like the internet, is only useful if people have access to it. Access to a computer would allow a recipient to view official information that was released by way of computer disk. Access to the internet would allow people wanting official information to search for it themselves on agency websites, possibly doing away with the need for an Official Information Act request. According to Statistics New Zealand, 47 per cent of households had a home computer in the year ended 30 June 2001. Just 37 per cent had access through that to the internet.[49] On the business side, in the same

---

46 Privacy Act 1993, s 6.

47 As mentioned, ss 6 and 9 of the Official Information Act 1982 provide reasons for withholding information under s 5 of the Act.

48 Te Puni Kokiri, Ministry of Maori Development *Maori Access to Information Technology* at <http://www.tpk.govt.nz/publications/subject/#it> (last accessed 5 January 2003).

49 Statistics New Zealand *Information Technology Use in New Zealand* at <http://www.stats.govt.nz/domino/external/web/prod_serv.nsf/htmldocs/Information+Technology+Use+in+New+Zealand:+2001> (last accessed 5 January 2003).

year, 88 per cent of private sector businesses in New Zealand regularly used a computer, and 80 per cent of businesses used the internet.[50] These usage rates are relatively high on a global scale, but there are nevertheless significant numbers of people in New Zealand without internet or computer access.

There is evidence to suggest that people on lower incomes are lagging behind in the adoption of new technology. More than 80 per cent of people earning more than $50,000 a year have internet access at any location, compared to just 47 per cent of people earning between $10,000 and $20,000 per year.[51] People living in smaller cities or towns are less likely to have home Internet access.[52] It also seems people with no tertiary qualifications have less access to the internet than their more qualified peers. Over 60 per cent of people who graduated from university had internet access at home, compared to 36 per cent of people with technical or trade qualifications.[53] There are also ethnic differences in household computer ownership; for example, 34 per cent of Maori households possess a computer, whereas the reported proportion amongst other ethnic groups is 60 per cent.[54]

It seems the provision of information via the internet favours those who are better paid, non-Maori, more qualified and living in cities. Technology, as well as enhancing society's access to information in general, also has the potential to widen the gap between the "information rich" and the "information poor".[55] All the computer-related technology in the world will not help people without access to a computer or the internet to better participate in our democracy. Therefore, we cannot rely totally on electronic access: there also need to be viable alternatives.

Within this, there is another possible problem: the compatibility of government information management systems with the systems of people who make Official Information Act requests. It is also possible that the form of electronic dissemination, if used as a way of releasing official information, may not help the recipient, given the diversity of software applications and versions available. The information technology industry has made quantum leaps in capability in short time periods, making it extremely difficult and expensive for consumers to keep up.

---

50 Statistics New Zealand, above.

51 AC Nielsen Netwatch 2000 Surveys, cited in Te Puni Kokiri, Ministry of Maori Development *Maori Access to Information Technology* <http://www.tpk.govt.nz/publications/subject/#it> (last accessed 5 January 2003).

52 People living in small towns reported the lowest levels of internet access (54 per cent) compared with 67 per cent in metropolitan areas: AC Nielsen Netwatch 2000 Surveys, cited in Te Puni Kokiri, Ministry of Maori Development, above.

53 Te Puni Kokiri, Ministry of Maori Development, above, 7.

54 Te Puni Kokiri, Ministry of Maori Development, above.

55 Australian Law Reform Commission *Open Government: A Review of the Federal Freedom of Information Act 1982* at <http://www.austlii.edu.au/au/other/alrc/publications/reports/77/ALRC77.html> para 2.6 (last accessed 5 January 2003).

In addition, recent discussions between the State Services Commission and the Ombudsmen have revealed that there is a need for the government as a whole to increase its understanding of the intention and administration of the Act.[56] Improvements in the standard of professional communication across government are also needed.[57] There was a concern that this had to be done before there could be any serious discussion of implementing a new Shared Electronic Environment (see below). This suggests that government departments may not be adequately taking account of their obligations under the Act when implementing information systems incorporating new technology. It is of concern that as technology advances at a quickening pace, some officials' understanding of the Act remains at a relatively elementary level.

The Ombudsmen's latest annual report has confirmed that the public sector generally has an inadequate understanding of the requirements of the legislation.[58] They say that given the length of time the Act has been in force, and its constitutional significance, we might have expected that its operation by now would be well understood. Unfortunately, the good progress being made with the dissemination of information, both voluntarily and in response to requests, is being offset by an inability or unwillingness by some to meet the statutory time lines.[59] This indicates that before there can be any potential reduction in time limits as recommended by the Law Commission,[60] some parts of the public sector need to be pulled into line and acquire at least a basic grasp of the workings of the Act. Disturbingly, lack of knowledge of the Act is preventing some of the potential benefits that technology can bring to its operation.

In addition to negative attitudes towards requests for information, the State Services Commission investigation also revealed that there were some negative attitudes towards new technology in public sector organisations.[61] While there are difficulties to be overcome in this area, they are no reason to sacrifice the major advantages the new electronic environment brings to the operation of the Act. Officials were also apparently aware that bringing more stakeholders, including the public, into decision-making through the use of technology could increase their workload: moreover, the timeliness element of policy development may be lost.[62]

---

56 Rose O'Neill and Sandi Beatie *Secure Electronic Environment – Phase 2* <http://www.e-government.govt.nz/docs/workspace-2> (last accessed 5 January 2003).

57 O'Neill and Beatie in "Chapter 3, Opportunities, Issues and Risks", above.

58 Annual Report of the Office of the Ombudsmen [2002] AJHR A.3, 10.

59 Annual Report of the Office of the Ombudsmen, above.

60 New Zealand Law Commission *Review of the Official Information Act 1982* at <http://www.lawcom.govt.nz> NZLC R 40 (last accessed 5 January 2003).

61 See generally, O'Neill and Beatie, above.

62 Ministry of Justice *Managing Your Information: Justice Sector Information Management Policy Guidebook* at <http://www.justice.govt.nz/pubs/reports/1997/infopolicy> (last accessed 5 January 2003).

It is important that issues like the above are resolved, in order to ensure the integrity of government information systems that employ the use of information technology, and to establish confidence in its reliability.[63] The next step is to examine the effectiveness of initiatives present in organisations subject to the Act.

V INFORMATION MANAGEMENT INITIATIVES

There is an overwhelming amount of material that organisations in the government sector can refer to when designing their information management systems. Three important initiatives are discussed below: the Ministry of Justice Policy Framework, the E-Government initiative incorporating several separate projects, and the Security of Government Departments Manual.[64]

A Ministry of Justice: "Managing Your Information"

In the late 1990s, the Ministry of Justice developed this Policy Guidebook[65] in conjunction with a group of public sector chief executives and other information management specialists. It is designed to improve the usefulness of information in the justice sector, but it has been suggested it would be appropriate for adoption by a wider range of organisations that are subject to the Act.[66] It is not aimed specifically at compliance with the Act, as much as good practice in information management generally. The specified outcomes of the process were: [67]

- to contribute to the effective participation of the people of New Zealand in the making and administration of laws and policies;
- to provide clear accountability of Ministers and officials for good government;
- to give confidence in the integrity of government and public decision making;
- to reduce the cost of government processes; and
- to support the efficient and effective management of government operations.

---

63 Michelle Barisic "Security and Privacy Issues Relating To Technology and The Law" <http://www.parliament.vic.gov.au/lawreform/tech/M%20Barrisic%20Art.htm> (last accessed 5 July 2003).

64 Archives New Zealand also has Record-Keeping Standards and a discussion document on Electronic Records (see <http://www.archives.govt.nz>). They need not be discussed here as they duplicate and complement much of what is discussed in Part V of this paper. Explicit reference is made in Archives website and documents to the Ministry of Justice Guidebook in particular, as well as the other initiatives mentioned here.

65 Ministry of Justice, above.

66 Interview with Andrew Jack, Privacy Officer, New Zealand Police (the author, 26 March 2002).

67 Ministry of Justice, above.

All of these have very clear links to the purposes of the Act set out in section 4. Of particular note for these purposes are the accountability and confidence in the integrity of government outcomes. These hark back to the Danks Committee's intentions in recommending the passing of the Act, and immediately provide a nexus between the implementation of the policy framework and the organisation's degree of efficiency and effectiveness in complying with the Act.

The framework was structured around several guiding principles – availability, coverage, pricing, ownership, stewardship, collection, copyright, preservation, quality and integrity.[68] The two key principles that have implications on the way organisations deal with Official Information Act requests are availability and coverage. The availability principle under the Policy Guidebook is that "Government departments should make information available easily, widely and equitably to the people of New Zealand (except where reasons preclude such availability as specified in legislation)".[69] This mirrors sections 4 and 5 of the Act. The Law Commission approves of this, as mentioned above, because the Act implicitly recommends that information be made available without being requested. This saves compliance costs in processing individual requests.

The coverage principle states that government departments should make information increasingly available on an electronic basis. In particular, published material or material already available publicly, policies that could be released publicly, information created or collected on a statutory basis (subject to commercial and privacy limits), documents that the public may be required to complete, and corporate documents in which the public may be interested.[70] Again, this is explicitly consistent with section 4 of the Act in that it advocates increasing the amount of official information available to the public.

Other basic principles outlined in the policy guideline include that there is a responsibility on government departments to employ good information management (the stewardship principle); and that government held information should be preserved only where a public business need, legislative or policy requirement, or a historical or archival reason, exists (the preservation principle).[71] The guidelines stress that information held by government must be accurate, relevant, timely, consistent and collected without bias. All of these guidelines reinforce ideas inherent in the Act.

The document is not merely a collection of principles. Specific checklists are also included in each area to help organisations put principles into practice. For example, there is a security checklist, covering all aspects of the life cycle of information, from creation, collection, use, storage and retrieval, and distribution, to retention and disposal. Finally, a set of policy statements is

68 Ministry of Justice, above.

69 Ministry of Justice, above.

70 Ministry of Justice, above.

71 Ministry of Justice, above.

included. These are meant to provide a starting point for various agencies to formulate their own information management policies.

In summary, if these guidelines were fully implemented in organisations who are subject to the Act, they would certainly have a positive effect on organisations' information management and help deal effectively with requests. Because of its broad ambit, the Policy Guidebook addresses security, threats, integrity of information, and classification. It also has a practical focus that would make it simpler to put into practice.

B E-Government Programme

This is a project spearheaded by the State Services Commission in 2000. It is still very much a work in progress. The idea behind it is to allow New Zealanders to access government services through the internet. It is said the initiative will improve both the quality of government and people's participation in government processes.[72] It includes the Secure Electronic Environment and the Centre for Critical Infrastructure Protection projects that are discussed in further detail below.

The project's mission is that by 2004, the internet should be the dominant means of enabling ready access to government information, services and processes.[73] Of the five key goals of the project, two are of particular relevance in this context – the provision of better, cheaper information, and greater participation by people in government. There is a clear link between these and section 4 of the Act, which outlines participation and the provision of information as two of the Act's purposes.

All of this sounds promising insofar as it implicitly promotes the purposes of the Act. However, the focus of the project is very much on the building of websites for public sector organisations. There are three key phases[74] to the project that aim to ensure that all such organisations have websites, and to progressively increase the capability of those websites. While this is admirable in that it ensures the essential advantages of the internet are going to be fully utilised, the people at whom this is aimed are not specified, and no consideration is given to their circumstances. This is acknowledged in the initial report. It notes that if the situation is left to develop on its own, it has the potential to divide society further in terms of those that have access to technology and those that do not. The strategy notes:[75]

The government must plan e-government in such a way that:

---

72 E-Government Strategy <http://e-government.govt.nz/programme/strategy.asp> (last accessed 5 January 2003).

73 E-Government Strategy, above.

74 E-Government Strategy, above.

75 E-Government Strategy, above.

- conventional means of access to government are maintained for those people who need them;
- community access to the internet is available for those people who, for any reason, can not access it from their homes; and
- educational and public information programmes are used to help New Zealanders, young and old, in using the new technologies.

However, the project does not address this issue itself; it has instead been left to an interdepartmental group within the Department of Labour, a part of the Community Employment Group.

1 Department of Labour: connecting communities

The rationale for this project is that any e-government initiative cannot be given its full effect if people do not in fact have access to computers or the internet. Experience with the adoption of information technology, as already noted, has favoured some groups of society over others. The project is designed to increase the ability of communities to access, participate in and efficiently use information and communications technology.[76] It recognises that it is the first concentrated effort of its type and that there must be co-ordination in central government assistance initiatives. Previously, there were many fragmented initiatives simultaneously being carried out by many different groups in society.[77]

The project also investigates some of the obstacles that stand in the way of having the whole of society internet connected. Barriers identified in the initial report include lack of information technology infrastructure, socio-economic barriers, cultural issues, lack of literacy and numeracy, and lack of technical support.[78] The project looks at how resources can be best allocated to overcome those barriers, and how strong links need to be formed between government, the community, and information technology and communications specialists.

The Connecting Communities initiative seems to be the only project making headway in ensuring that technology can be taken advantage of at a grass roots level, and for this reason it has an extremely important role in any discussion information technology in government.

2 State Services Commission: shared electronic workspace

This project examines the possibility of a shared electronic workspace between government departments. Especially relevant functions of such a system in terms of the Act would include the

---

76 Community Employment Group *Connecting Communities* <http://www.dol.govt.nz/cegccstrategy.asp> (last accessed 5 January 2003).

77 Community Employment Group, above.

78 Community Employment Group, above.

ability to track versions of documents, the ability to trace security breaches, access to a single departmental contact point for information filtering, and the ability for a wider stakeholder group to have access to information generated.[79]

There was an acknowledgment by the authors of the project report that policy development can be a very complex process.[80] Parties in public service organisations consulted by the authors saw greater utilisation of technologies as necessary "to improve the quality and efficiency of government", and "to complement and keep pace with", the move to utilise advanced technologies for greater engagement between citizens, businesses and government.[81] Again, the implications of such technology for the Act, although not directly referred to, are indirectly acknowledged at the outset.

The basic advantage of the Secure Electronic Environment in terms of official information is that it would allow more confidence in the integrity of information. With version control, there can be assurance that the version released as official information is the version retained by the department or organisation. Also, there can be more confidence that the same information is consistent across the organisation. There may be a lesser chance of security breaches and manipulation if there is a centralised system for keeping control over information. Such a security system must be less complex if one system controls all electronic information that the government holds. There would be a greater chance of electronic information being made available without being requested, which as noted previously is consistent with the policy of the Act. Common databases also make retrieval of information easier and increase ease of access. All these things imply efficiency and cost savings.

The Ombudsmen considered that the major reason for current delays in responding to requests relates to the failure of recipients to determine who should be responsible for processing it.[82] If there was to be a central electronic store of information under this initiative, it may no longer be an issue who holds the particular information. It may also overcome any concerns caused by privacy requests being handled by a number of organisations rather than just one. In combination with a greater understanding on the part of officials of how the Act works, this may lead to a reduction in processing times.

---

79 Rose O'Neill and Sandi Beatie *Secure Electronic Environment – Phase 3* <http://www.e-government.govt.nz/docs/workspace-3> (last accessed 5 January 2003).

80 O'Neill and Beatie, above.

81 Rose O'Neill and Sandi Beatie *Secure Electronic Environment – Phase 2* at <http://www.e-government.govt.nz/docs/workspace-2/> (last accessed 5 January 2003).

82 Annual Report of the Office of the Ombudsmen [2002] AJHR A.3, 10 <http://www.ombudsmen.govt.nz/annual.htm> (last accessed 5 January 2003).

3 Government Communications Security Bureau: centre for critical infrastructure protection

One of the Bureau's functions is to assist Government departments and agencies to protect their electronic information resources and communications systems. Essentially, the function of the GCSB that relates to information systems security is about the protection of information that is processed, stored or communicated by electronic means. It includes the formulation of communications and security policy; the promulgation of standards; the provision of material, advice and assistance; and assessment and inspection services to government departments and authorities.[83]

The GCSB performs this function in two ways. The first is via the Centre for Critical Infrastructure Protection. This is dedicated to providing advice and support to protect critical infrastructure from cyber threats, helping to prevent damage that may be caused through misuse of the internet.[84] Research has shown that there are various cyber risks to infrastructure, including lack of management-level understanding of the need for audited information technology security measures, and the challenges facing information systems administrators who need to maintain security as vulnerabilities continually emerge in widely-used software.[85]

Secondly, it publishes the New Zealand Security of Information Technology Publications. The GCSB publishes this series to provide "guidelines to New Zealand government organisations in support of securing information technology systems and protecting the associated information and services".[86] The publications contain detailed analyses of the threats to the integrity of information that government agencies hold, and advice on how to reduce the risk. Generally, information technology security issues are comprehensively dealt with.

Insofar as the GCSB focuses on security of information technology, its objectives are achieved appropriately. It provides for protection from cyber risk, and covers confidentiality, availability and integrity of information generally. Because it addresses security issues, it may help stop the unintended release of information protected under sections 6 and 9 of the Act, although this is not separately considered.

---

83 Government Communications Security Bureau <http://www.gcsb.govt.nz/infosec.htm> (last accessed 5 January 2003).

84 Centre for Critical Infrastructure Protection <http://www.ccip.govt.nz> (last accessed 5 January 2003).

85 Cabinet Paper *Centre for Critical Infrastructure Protection* <http://www.ccip.govt.nz/about-ccip/cabinet-paper.htm> para 6 (last accessed 5 January 2003).

86 Government Communications Security Bureau, Security of Information Technology <http://www.gcsb.govt.nz/nzsit> (last accessed 5 January 2003).

C Security of Government Departments: Department of Prime Minister and Cabinet

The Interdepartmental Committee on Security publishes a manual setting out minimum standards that must be adopted by all government departments, ministerial offices, the Police, the Defence Force, the New Zealand Security Intelligence Service and the GCSB.[87] It is also made available to Crown entities and state-owned enterprises to help them to meet their obligations under the Act.[88] The rationale behind it is to have a consistent set of information security guidelines for the government sector. The policy statement of the manual stresses the importance of safeguarding resources and information to the extent consistent with the public interest and personal privacy[89] – so again, the language mirrors that of the purpose statement of the Act.

Policies are set out in the manual, and a risk management approach to security is advocated.[90] Throughout the manual, the reader is referred to guidelines set out by the GCSB, and other organisations for the practical application aspect, such as the New Zealand Security Intelligence Service. Resources that contribute to the debate are thoroughly canvassed. Both electronic and non-electronic forms of information are discussed. On the whole, the manual makes a useful contribution in that it attempts to pull all of the initiatives together to make a comprehensive whole.

D Potential Deficiencies

The various initiatives do have their drawbacks. One important aspect is that none of them are binding. As noted at the beginning of this section, there is a wealth of information available to organisations about information technology, and how best to implement it and guard against risks. The question becomes one of priority – how can we, as citizens in a liberal democracy, be sure that the public sector is using technology to its best advantage for our benefit? Lack of enforceability strongly limits effectiveness.

Furthermore, access of various segments of society to information technology seems to have fallen by the wayside in many government projects. It has been left to a relatively tiny part of the public sector as a problem to solve, when in reality, it should perhaps be the foremost consideration. After all, the public sector is meant to work for the citizens of New Zealand, including the voting public. It is arguable whether a small group within one government department has enough influence and resources to be able to have a decent attempt at overcoming this obstacle. It should perhaps be dealt with by a more central agency, such as the State Services Commission.

---

87 Department of the Prime Minister and Cabinet *Security in the Government Sector* at <http://www.security.govt.nz/sigs/index.html> (last accessed 5 January 2003).

88 Department of the Prime Minister and Cabinet, above, ii.

89 Department of the Prime Minister and Cabinet, above, 1-2.

90 Department of the Prime Minister and Cabinet, above, 1-3.

In most cases, it seems as though the parties developing the initiatives have not directly considered the Act. There is very little explicit reference to it. This is of concern, as any change to the way information is created, collected, stored, disseminated or disposed of must have implications in terms of this central piece of legislation. It seems that public sector officials have not adopted the principles behind the Act half as enthusiastically as the courts, who have gone so far as term it 'constitutional' in nature.[91] Perhaps the underlying problem is its lack of prominence in the thinking of those responsible for official information, or a lack in understanding of the Act on the part of officials.[92]

VI CONCLUSION

Technology like the internet and the widespread use of computers, has the potential to add immense value to the purposes and operation of the Act. Technology enables organisations to store more information than previously, and retrieve and disseminate it more quickly.

There have been solid, valuable attempts by various public sector groups in recent times to overcome problems associated with rapid technological change. Examples include the E-Government project, and more localised initiatives in certain parts of the public sector. Taken together, they go a significant way towards addressing those problems.

However, two major difficulties remain. The first is that not enough emphasis seems to be being given to improving the access that some segments of society have to technology. It is suggested that more of a central, co-ordinated effort needs to be directed toward this end. In the final analysis, it is the people of New Zealand benefit from the effective operation of the Act, and their needs should be given more emphasis.

Secondly, co-ordination between various initiatives to improve information management systems in government does not seem to be effective. There are many guiding resources and it is not always clear which one should be followed by which organisation. While individual initiatives taken as a whole address most of the concerns, this patchwork approach is arguably not appropriate when it has implications for such important, constitutional legislation. A worrying lack of understanding of the Act, or a negative attitude towards technology on the part of public officials, may be exacerbating this problem.

It is suggested that a co-ordinated, educational approach be taken by central government to ensure that the benefits citizens gain from the Act are not undermined by technological change, but enhanced.

---

91 *Commissioner of Police v Ombudsman* [1988] 1 NZLR 385, 391 (CA) Cooke P.

92 Annual Report of the Office of the Ombudsmen [2002] AJHR A.3, 10 <http://www.ombudsmen.govt.nz/annual.htm> (last accessed 5 January 2003).