Privacy issues and new technologies*

SUE COLMAN
Senior Policy Officer, Office of the Federal Privacy Commissioner

Among the many challenges posed by new information and communications technologies is to address the question of what it all means for individual privacy. Far-reaching changes to the way we communicate with each other, with organisations and with the world at large are presently being ushered in, and some of these have quite significant implications for our personal privacy. While it is true that cultures are changing, I suggest there are parts of the present culture that we should aim to preserve. Personal privacy is one of these.

The right to privacy is such a basic, universal expectation, that it is rarely as clearly articulated as it is felt, and rarely more keenly felt than when it is threatened. But how do we protect it in the face of fundamental changes to our modes and means of communication? How can we avail ourselves of the best that the technology has to offer without at the same time losing autonomy, anonymity, and choice over who knows us and what we're doing? Privacy in the context of new technologies is very much about how we define ourselves as we interact with others via complex electronic systems and connections.

A conscious effort is required to ensure we do not gradually and unwittingly accept a diminution of our privacy rights. Universities, as significant users of new technologies, need to assess the privacy implications of using new technologies by asking: What does it mean for the individual? Does it reduce or support individual autonomy, choice, sense of security, trust? What information does it generate about individuals and how is it used? What controls exist to protect the integrity of the transaction?

Ideally, this assessment should take place before the event; if not there is a chance that any infringements on privacy will slow the pace and extent to which the new service will be embraced by the very communities they are designed for. In any case, the assessment should not take place only once, but be a continuing appraisal of the impact on our private lives. To quote David Flaherty, formerly a leading privacy scholar and now the Information and Privacy Commissioner of the Province of British Columbia:

> *Users of telecommunications services and digital commerce need to reflect on a regular basis on the privacy implications of the technology that they happen to be using in any aspect of their professional or personal lives (which technology, like the Internet, is in fact becoming more and more intertwined as the distinction between home and workplace becomes more blurred).*[1]

The need to protect our privacy, particularly in the light of the take-up of new technologies, is one of the reasons why the federal government has proposed to extend privacy protections to the private sector. In September 1996 the federal Attorney-General released a Discussion Paper, "Privacy Protection in the Private Sector", which sets out one possible framework for a private sector privacy regime. (The Discussion Paper is available on the Internet at http://www.agps.gov.au/customer/agd/clrc/privacy.htm.) Tertiary institutions, as significant users of new technologies and as holders of large amounts of personal information, will no doubt be interested in the outcome of this current review.

Public concerns about personal privacy

Opinion polls show that the public is increasingly uneasy about the effect of modern technology on privacy. In 1990, 67% of the people interviewed said privacy was a very important social issue. Four years later it was 75%. People feel that governments can learn anything about them. They also tend to have less trust in the way commercial organisations handle their personal information than government or professionals.

Among the reasons for the increased concern is developments in information technology. 6 in 10 people believe they have lost control over how their personal information is used and who it is passed on to. People resent unwanted intrusions from mail and telephone marketing companies. More than 9 in 10 think organisations should get their permission before passing on their information to somebody else.

Against this backdrop we need to consider the effects on personal privacy of new technologies and the way they have been applied to the services we now receive. Networked information and communications services, smart cards, calling line identification, and data warehousing are making possible new ways of personal and commercial interactions, the effects of which are still to be fully understood. Australians have been eager to take up electronic banking, new telecommunications services, EFTPOS, the Internet, and we can reasonably expect a strong take-up of the full range of interactive services promised by the roll out of fibre optic cable.

*This article is based on an address given to "New Technology and Tertiary Education: Changing the Culture" seminar held 11 July 1996, Storey Hall, RMIT, Melbourne.

Most of these provide a means of communication, or a means of accessing information. They generally require the user to identify themselves to gain access and records are usually generated about the transaction. People's participation and use, therefore, leads to a data trail about them.

Data trails

Most people are unaware of the extent to which their use of electronic systems is recorded. There are virtually no online activities or services that guarantee an absolute right to privacy. It is now possible to monitor people's use of the World Wide Web. A Californian software company is developing software specially for employers that will allow tracking of every WWW site, news group or file transfer location visited by employees, and record the size of each file downloaded. The company promotes the software in the following way:

> *We're giving employers something like an itemised phone bill ... The spinoff is that they can see what the employees are doing.*[2]

There are also commercial incentives to record people's use of the Internet. Some companies are reportedly logging e-mail addresses to help gauge the effectiveness of advertisements they pay for on other organisations' web sites. At the same time they can chart how customers move through web sites and find out what type of computer they have and the speed of their connection.[3] Qualitative information can also be obtained. Information generated as a result of people's visits to web sites enables quite detailed profiles to be compiled about users' needs, habits and purchases. Most people would have no prior notice that this occurred. Interestingly, some of the larger service providers are now offering on-screen notice and opt-out options for people who prefer not to be approached with marketing offers and the like as a result of their use of online services.

A new technology from Netscape, called Cookies, allows a server to download a cookie with a secret code into a user's web browser for storage on their PC. Web sites are thus able to mark their readers with what has been described as an indelible marker. "Each time you revisit the web site, the server will know that it's you."[4]

Expectations of anonymity and confidentiality

The capacity of new technologies to record our activities challenges our expectations of anonymity and confidentiality. Whereas new technologies are offered to us as new and better ways of doing essentially the same things we have always done, they are in fact changing the fabric of our communications.

Most of us have expectations that our private communications will remain private. However, how can we know, now, what is private and what is public? While we may use e-mail in the same way as we pick up the telephone or write a letter, we cannot be sure that such a communication will be limited to the person of our choice. Electronic mail via the Internet is generally understood as being inherently insecure, as are the accompanying information storage systems. And contrary to many people's expectations, items posted to chat groups or newsgroups may not be anonymous. As noted by an international grouping of Data Protection Commissioners considering data protection issues on the Internet, "Never send or keep anything in your mailbox that you would mind seeing on the evening news."[5] The growing use of the Internet and e-mail in universities, by both staff and students, would suggest that these problems will become of increasing importance for educational institutions in the future.

Even the privacy of our telephone conversations now seems to be at risk. A newspaper article in April 1996 heralded the arrival onto the Australian market of a telephone call recording device which could be activated by one of the parties at the push of a button, without the other party having to consent to the recording.[6]

An article in LASIE journal in 1995 raised the interesting scenario of the potential breach of confidentiality that can arise in connection with a library undertaking reference searches, using online technology, on behalf of a client. The writer noted that a librarian could breach a person's expectations of confidentiality by posting difficult reference queries over the Internet, thereby exposing the identity of the enquirer and the nature of their query.[7] This is a good example of how the medium of communication can alter the intent and scope of the communication itself.

New services such as the Internet also challenge our notions of what is public and what is private information. An example was the issue reported in the press during 1996 of the making available of family court judgments over the Internet. Certainly, there are significant advantages to the community in making legal proceedings more open and accessible. However, the problem here, from a privacy perspective, is that making the information available over the Internet greatly increases the potential for the information to be searched, scrutinised and used for a much wider variety of reasons beyond the purposes for which it was published in the first place. This means that there could be a need to seriously consider de-identifying the information to protect the privacy of the individuals concerned, who otherwise could be targeted by Internet users for quite unrelated and unwelcome purposes.

Of course, it is not only our interaction with the Internet that raises privacy concerns. Intelligent systems used by libraries allow our borrowing histories to be recorded. Smart card technology which uses an in-built computer chip, and which has been trialed in Australia on a number of occasions, has significant information storage capacity. If used in daily contexts such as shopping and using public transport, quite detailed pictures could be developed about those day to day activities we normally regard as private. Our preferences and choices can be easily recorded using such technologies. They result in identifying us when ordinarily we would be anonymous. This is not to say that there is anything inherently valuable about anonymity *per se*, but it could be argued that there is a certain freedom that comes from not having to identify ourselves before engaging in such basic activities as shopping, moving around, and other public interactions.

Anarchy on the Net

Another difficult issue surrounding the use of the Internet is that standards of behaviour and data management practices cannot be imposed by laws, nor, indeed, by any means. There is no overall responsibility assigned to a single body and there is no international oversight mechanism to enforce any legal obligations which might be directed to its use. Essentially, then, control of the Internet is left to whatever national controls governments can persuade users to accept and/or norms of behaviour developed by the users themselves.

It is clear, also, that the Internet poses special challenges to those who would seek to apply traditional privacy principles to it. Notions of responsibility, ownership of information, control over its dissemination, people's awareness of collection of personal information, knowledge and consent as to its use and disclosure sit uneasily alongside the operating environment of the Internet.

Security concerns

Security is a key feature of privacy protection in the electronic environment. Information systems need to be designed in such a way that they give effect to broader information handling policies. Questions about who has access to information, how it may be used, and whether it can be disclosed, need technical as well as policy responses. Also, people's willingness to embrace new technologies will largely be determined by their level of confidence in the security aspects of new systems.

As we use electronic commerce more and more we will need to develop trust in payment systems and how our private financial information will be protected against unauthorised access and use. Authentication techniques will need to be robust. Developments in digital signatures, iris recognition, retina scans, voice recognition and keystroke recognition are among the new ways of confirming our identity and protecting our information in the use of new systems. However, the ethical implications of these new-generation identification systems need to be kept in mind so that we don't become slaves to them and, in the process, undermine fundamental freedoms.

Database developments

New database technology now makes possible the collection, aggregation, manipulation, massaging and disposal of vast quantities of information. When this is personal information, it threatens our ability to control what others know about us. It threatens our uniqueness. This could have various implications in the university context.

Student records are a potentially sensitive class of personal information. From a privacy perspective, they should not be used for any purposes beyond the purpose of collection.

An article in a privacy journal earlier this year noted that the University of Delaware in the United States has set up a system whereby any student by producing a personal identifying number, may access his or her grades, class schedule, financial aid information and unofficial transcript on a World Wide Web site created by the university. Digitised photographs of students are available online to administrators and to the individual students, but not yet to faculty members or fellow students. The data is encrypted and student ID numbers and PIN numbers are required to access individual records. Registrars and information specialists on other campuses have expressed concerns about the possibility for breaches of confidentiality or other misuse in such an environment and a task force is presently further studying the issue.[8]

An Australian university recently sought the advice of the Privacy Commissioner's office about the practice of publishing student results in a public place at the university showing student ID number. The practice raised privacy issues because students at the university were able to use the ID number to find out the name of the student associated with that ID number by using the university's e-mail facilities. This practice would not have been possible in the days when such technology was not available to students and others.

There are many other types of sensitive information in the possession of universities, and it does not take a great deal of imagination to understand the privacy implications of improper access to or use of such information when it is contained in databases and accessible through internal (and external) networks. Information likely to be collected includes:

- Academic records;
- Enrolment details, including previous education, employment, family information and financial information, including whether receiving government benefits;
- Times of classes and lectures attended and where;

- Records of involvement in extra-curricular activities and clubs, such as student union and political groups;
- Library records;
- Student counselling files;
- Records of access to online services, including the Internet;
- Health and medical records;
- Details of complaints or grievances which may be lodged by students;
- Personnel records and employee files, including details of contracts with academic staff.

Each of these categories of information may have been given or gathered free of privacy concerns, yet if all this information is brought together, it has the potential to create a very detailed picture of an individual that he or she would not have anticipated when the information was given. Also, people giving information have certain expectations about the way it will be used, and therefore these expectations must be recognised in a formalised way, for example in the form of an internal privacy policy within institutions.

Some readers may be aware of the controversy which arose in early 1996 surrounding the introduction of a smart card (the QuickLink card) by the student union at the University of Newcastle. The card served as the union membership identification card and also had to be presented to obtain discounts and privileges which are accorded to students as union members. Students expressed concerns, in particular, about the lack of choice in having to have such a card, and also about the implications of their personal membership details being kept on a database associated with the scheme (as reported in the press). The card has since been withdrawn from use.

What can be done to protect privacy?

Fair information handling practices of the type found in the *Privacy Act 1988* and in the *OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data* provide a framework for developing information systems which protect individual privacy.

Organisations such as universities need to ask themselves beforehand:

- What information do we gather?
- Is it necessary?
- What do we do with it? For what purposes is it used? What controls/limits are there on use? Is use with the consent of individuals?
- What controls are there on improper or inappropriate disclosure of information?
- What possibilities are there to provide individuals with choice?

Overlaying these issues upon the technological environment, institutions should be exploring ways of offering better privacy protection around their use of systems. They include encryption systems, enhanced password protection, anonymous use of systems where possible, and clear separation of transaction data from content data.

Institutions should use privacy impact statements to assess the possible privacy implications associated with a new technology before it is introduced.

Importantly, good information handling practices need to be developed. Universities need to take active steps to encourage awareness among the community, students and staff, about privacy issues associated with their use of technology. If it is not possible to offer guarantees of confidentiality, people should be made aware of this so they can decide what kind of information they may communicate via differing media. Use of personal information gathered in the university context must be limited to the purpose for which it was collected and must not be generally disclosed without the individual's consent.

Issues to consider in establishing a privacy policy for online services

A useful set of standards to protect privacy in the online environment has been developed by a grouping of Data Protection Commissioners in Germany.[9] They may provide a starting point for universities in addressing privacy issues within their own environment. The main aspects of that framework are reproduced below.

1. *Anonymous use or sparing use of data*: Online services should be designed so that as little data as possible is collected, processed and used. Anonymous use and payment forms should be offered. If completely anonymous use is not possible, the use of pseudonyms may be considered, and identifying the user should only occur if there is substantiated legal interest in the identification.

2. *Basic data*: This should only be collected, processed and used as necessary for the substantiation and management of a contractual relationship and for system maintenance. It can be used for advertising and market research if the individual has not objected, but can only be disclosed to third parties with express consent.

3. *Connection and billing data*: The use of this kind of information should to be limited to the purpose of conveying offers and for billing purposes and should

be deleted when it is no longer required. Storage of billing data should not allow recognition of the time, duration, content etc of specific communications and connection and billing data may only be used for the purposes for which it is recorded, unless express consent is given.

4. *Interaction data:* Interactive data may only be collected with the knowledge and express consent of the individual, and may only be processed and used for purposes limited to the purpose for which it was collected. (Interaction data is data, for example, which is entered while searching encyclopaedias or in online games.) Similar restraints apply as above.

5. *Consent*: A contractual relationship must not be made dependent on the individual concerned consenting to the processing/use of personal data outside of the permissible purposes for which it was recorded. If any data is collected on the basis of consent, consent may be withdrawn at any time. A minimum standard of consent must be defined - including the consequences of consent and the right to withdraw consent and people must be able to access consents, conditions of service etc.

6. *Transparency of the services and control of the data transmission by the participants*: The automatic transmission of data is to be restricted to the amount necessary to fulfil the contract, and any transmission beyond that requires special consent. With this technology, participants must be informed that their data is to be transmitted and stored when using electronic services and be able to stop the process at any time. The user software must be able to be activated by the user to record the flow of data. Service providers must not use any recognisably insecure networks, and state of the art processes (e.g. in cryptography) are to be used.

7. *Rights of those affected*: Individuals must be given access to information, and to blocking, correction and deletion of information.

8. *Data protection inspection*: Effective, independent and permanent data protection supervision is to be guaranteed.

10. *Data protection regulation*. Regulation capable of dealing with cross-border services is necessary. In the short term persons affected must be given suitable means to uphold their data protection rights.

Interestingly, some of the overseas sources of advice on privacy protection also refer to the obligation resting on individuals in relation to protecting their privacy as they interact with new technologies.[10] The Information and Privacy Commissioner of the Province of British Columbia encourages individual users to become sensitive and aware users and to engage in self protection.

> *Individuals have to come to grips with the surveillance capacity of retail credit cards, automated teller machines, electronic cash transactions, various interactive services, telephone calling cards, cellular telephones, the proliferation of other unique identifiers, and smart cards.*[11]

But he also says that the Internet community needs to promote even more of a culture in which the tracking of digital footprints, by whatever method, is illegal, immoral and unethical without individual consent.

We are all sailing on unchartered waters when it comes to finding ways to protect intangible values, such as privacy, in the equally intangible realm of cyberspace. But we should not be deterred from the attempt. It is vital to ensure that we as individuals control the social effects of these technologies and not the other way around.

Endnotes

1. David H. Flaherty, PhD, Information and Privacy Commissioner, Province of British Columbia, 'Some reflections on privacy in electronic communications with special reference to the Internet and the situation in British Columbia', *Special Colloquium on "The Internet: Beyond the Year 2000,* University of Toronto, April 28-May 1, 1996.

2. Quoted in *Privacy Times,* May 17, 1996, p.9.

3. See *Privacy Journal*, February 1996, p.5.

4. See *Privacy Journal*, February 1996, p.5.

5. International Working Group on Data Protection in Telecommunications, *Data Protection on the Internet: report and guidance,* 21 May 1996.

6. Reported in *The Australian*, April 16, 1996, p.49.

7. Pace, Leslie, "Privacy on communications networks", *LASIE*, Vol 25, Nos 4 & 5, pp 72-3.

8. 'Student Info in Cyberspace', *Privacy Journal* March 1996, p.1.

9. These standards come from Germany and are the result of a resolution agreed to at the Conference of Data Protection Commissioners of the Federation and the Laender. The standards were brought forward for discussion at a meeting of International Data Protection Commissioners held in Budapest on 15-16 April 1996. The resolution is entitled *Resolution of the Conference of Data Protection Commissioners of the Federation and the Laender of 29 April 1996 on key points for the regulation in matters of data protection of online services.*

10. See Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force *Privacy and the National Information Infrastructure: principles for providing and using personal information*, June 6, 1995, particularly Principle IIIA.

11. David H. Flaherty, PhD *op cit.*