Prometheus, Vol. 18, No. 2, 2000

Privacy Protection—A New Beginning?[1]

MICHAEL KIRBY

ABSTRACT *Privacy is universal value. But according to* The Economist *in 1999 it is finished—killed off by the remarkable capacity of information technology to analyse, trace and re-assemble personal data: affording an unprecedented insight into individual attitudes and activities. Based on the progress made in implementing the* OECD Guidelines on Privacy *(1980), the author, who chaired the OECD group that devised those Guidelines, reviews their impact, the need to update them and contemporary proposals for new privacy protections suitable to the current technologies. He concludes that the capacity to uphold human values in the context of new technologies, such as informatics and genomics, presents one of the largest ethical questions for the 21st century.*

Keywords: information technology, privacy, OECD guidelines on privacy, revision of OECD guidelines, privacy seal, human genome and privacy, genetic privacy, democratic governance and technology.

OECD Principles: Twenty Years On

The OECD Principles on Privacy had an importance extending far beyond their subject matter.[2] They concerned the capacity of law-making institutions in democratic societies to respond to large and complex developments in global technology.

Let me remind you that this was a novel initiative for that hard-nosed international body of economists and statisticians. The OECD had grown out of the Marshall Plan by which the economies of Western Europe had been rescued from devastation after the second world war by the drive, generosity and capital of the United States of America. As such, the OECD was not a body concerned with human rights. It could leave such nebulous and contentious topics to the Council of Europe, the European Court of Human Rights or the never-ending debates in the United Nations, including its agency UNESCO, meeting in Paris on the other side of the River Seine.

The concern which propelled the OECD into the issues of privacy was the fear that its member states would introduce incompatible and conflicting laws for the defence of privacy in the newly established data bases of the interlinked information technologies. The fear that this would result in serious barriers to the generally free flow of data across the borders of the member states of the OECD, and beyond, was the cause that brought together the Expert Group on Privacy which I was elected to chair.

That we achieved consensus in the end was a remarkable tribute to the outstanding work of the OECD Secretariat, led for this project by Mr Hans Peter Gassmann. Within the Expert Group there were brilliant antagonists. The chief United States delegate (Mr William Fishman) expressed with great clarity the American commitment to the free flow of data and of ideas. The head of the French delegation (Mr Louis Joinet) led those in

ISSN 0810-9028 print; 1470-1030 online/00/020125-08 © 2000 Taylor & Francis Ltd

the Expert Group who were alarmed by the dangers to individual privacy of completely unrestrained collections of personal data, vastly expanded in quantity and kind by the new technology. Each protagonist spoke with sincere conviction and gathered supporters. The contemporary state of technology meant that United States business interests stood to gain from the growth of informatics and the spread of trans-border data flows, while the French and European business interests, on the other hand, coincided generally with restrictions insistent upon privacy protection. Not for the first time philosophy and law followed trade.

It is something of a miracle that the OECD Guidelines emerged at all, but they were able to draw on the work of the Nordic Council[3] and the Council of Europe.[4] The Guidelines gave depth and substance to the generalised statements about privacy in the international[5] and regional[6] statements of human rights. Not that these guarantees have proved ineffective. On the contrary, the guarantee of private life in the European Convention was to be pressed into service to remove the criminalisation of homosexual conduct in Northern Ireland,[7] the Irish Republic[8] and Cyprus.[9] The guarantee of privacy in the *International Covenant on Civil and Political Rights* was invoked to precipitate the removal of Australia's last criminal laws against private adult consensual homosexual conduct.[10]

Once adopted, the OECD Guidelines became highly influential on a broader plain throughout the member states of that organisation. Thus the Australian[11] and New Zealand[12] statutes were profoundly influenced both by the privacy principles expressed in the Guidelines and by the high measure of flexibility which they suggested to be appropriate to each jurisdiction introducing them into its laws and practice.

A review of the New Zealand Act, after its first 3 years of operation,[13] found no substantial faults with the 12 information privacy principles contained in the Act, adapted from the OECD Guidelines. One commentator observed:[14]

> That the original set of principles has largely stood up to 5 years of experience, in a myriad of different sets of circumstances and still looks pretty good … must be seen as a solid endorsement of the decision to follow some other jurisdictions in enacting principles as such rather than attempt to reduce them to a set of precise and prescriptive rules. This is, of course, a credit to the good sense and scope of the original OECD principles and perhaps especially the 1988 Australian embodiment of them, upon which the NZ set was closely based. It is also a credit to Bruce Slane, who devoted the better part of the 1992–93 year to trying to get the NZ Act right.

Since the 1980 Guidelines on Privacy, the OECD has moved increasingly to a recognition of the close inter-relationship between an open and dynamic economy and an open and dynamic democracy operating under the rule of law. This has led the OECD, like the World Bank, into an increased appreciation of the importance of governance to economic development and hence of good governance in developing countries for the growth of global markets upon which depend the sustained economic viability and strength of the economies of OECD member states.

It was therefore unsurprising that, in October 1998, at Ottawa in Canada, the OECD convened a high level meeting of Ministers and officials from the 29 member countries to consider, amongst other things, the privacy questions presented by the continuing rapid growth in electronic commerce.[15] Once again, it was a technological development with huge economic ramifications which had propelled the OECD into concerted action. Once again, in the words of the OECD Secretary-General, Donald Johnston, a major goal was to 'lay down a rules-based framework to eliminate, or reduce, the downside risk' perceived in electronic commerce.[16]

As a result of the Ministerial meeting, three declarations were adopted to establish baseline principles and goals and to provide guidance on the future work of the OECD.[17] One of these, the *Declaration on the Protection of Privacy on Global Networks,* recognises the ubiquitous nature of digital computer and network technologies today. They offer the opportunity for great social and economic benefits towards information exchange, consumer choice, market expansion and continuing innovation, but they present problems for the fair collection and handling of personal data.

The Ministers in Ottawa recognised that the 1980 Privacy Guidelines of the OECD were still applicable in that they 'represent international consensus and guidance concerning the collection and handling of personal data in any medium, and provide a foundation for privacy protection on global networks'.[18] The Ottawa Declaration affirmed the commitment of the governments of OECD member countries 'to the protection of privacy in global networks in order to ensure the respect of important rights, build confidence … and prevent unnecessary restrictions on transborder flows of personal data'. They saw this as a way to 'build bridges between the different approaches adopted by member countries to ensure privacy protection on global networks based on the OECD guidelines'.[19] The Declaration also recognised that different countries would implement privacy protection by legal, self-regulatory, administrative or technological means. However, the Ministers considered it important to encourage the adoption of privacy policies, the notification online to users of privacy policies, the promotion of user education and the encouragement of privacy enhancing technology.[20]

Although many users of information technology come from countries outside the OECD, Hong Kong is an Associate Member, Japan, Korea, Australia and New Zealand in this region are members, and the advanced economies of the OECD undoubtedly dominate information technology, transborder data flows and global networks. So the Ministerial Declaration on Privacy is important. It signals a continuing commitment of the OECD to the protection of individual privacy. This unexpected child, conceived in a union of economics and human rights, born in 1980, is now 20 years old. Its parents have acknowledged and praised it, yet the world of today, particularly the world of technology, has changed beyond recognition from the world into which it came nearly 20 years ago. It is timely to consider the changes and some of their implications. It is timely to ask, as the *Economist* did in May 1999: are we witnessing 'the end of Privacy'?[21]

Cyberspace and Electronic Commerce

The most important change is brought about by the growth of the World Wide Web, the unstoppable expansion of the Internet and the rapid development of e-commerce. Use of the World Wide Web doubles every 12 months.[22] William Gibson's vision of cyberspace[23] appears to be fast becoming a reality. Starting in 1995 with 8.5 million users, the Internet is expected to reach over 142 million users by the year 2000.[24] Looking ahead, it is necessary to envisage the way in which the lives of human beings will be altered as the global network of interconnected users of information technology becomes bigger and ever more powerful.

A recent OECD document[25] listed 92 ways in which, it was claimed, the lives of ordinary people will be changed by the technology over the next 30 years. Global culture, education, employment, production and even crime will be affected. Privacy, it is argued, will be harder to maintain. Not unconnected with this, interpersonal relationships of human beings may become increasingly unstable. National governments will have limited control over cyberspace and over the pace at which globalisation of inter-connected human consciousness is occurring.

Whereas in the past one of the chief protections for privacy lay in the sheer cost of retrieving personal information (and the impermanency of the forms in which much information was stored) such practical safeguards for privacy largely disappear in the digital age.[26] It is not always appreciated by users of the Web that without specific initiatives on their own part, their visits to particular websites can often be resurrected, presenting a comprehensive profile of their minds. That profile may illustrate the subjects in which they are interested: their inclinations, political, social, sexual and otherwise.[27]

The extensive indexes on Internet sites such as Yahoo[28] and the Altavista search engine[29] change forever the personal information profile of the individual. The OECD Guidelines of 1980 were prepared in the context of the technology then known and envisaged. However, that was long before the Internet and the web crawlers, spiders, robots and trawlers which have introduced completely new methods for an intense dataveillance of the individual.[30]It is in this context that there appears to be a need to review the 1980 OECD Guidelines, which are already showing signs of their age. Informed writers are already suggesting the necessity for new privacy principles apt to contemporary technology. The suggestions include:

1. a right not to be indexed;
2. a right to encrypt personal information effectively;[31]
3. a right to fair treatment in key public infrastructures so that no person is unfairly excluded in a way that would prejudice that person's ability to protect their privacy;
4. a right to human checking of adverse automated decisions and a right to understand such decisions;[32]
5. a right, going beyond the aspiration of the 'openness principle', of disclosure of the collections to which others will have access and which might affect the projection of the profile of the individual concerned.[33]

The common theme of many of the suggested revisions of the OECD Guidelines is the need to render 'data collection practices … fully visible to the individual … Any feature which results in the collection of personally identifiable information should be known prior to operation and … the individual should retain the ability to disentitle the feature if he or she so chooses'.[34] Some might consider this too absolute a statement of disengagement. Others might question the marginal utility of undemanded notifications of all identifiable information about the individual without any initiative on the part of that individual. Yet clearly the 'openness principle' of the OECD Guidelines was always one of the weakest. The advent and potential of the Internet require that there be new attention to it.

Similarly, the rapid growth of e-commerce has led to demands not only for national laws and self-regulation but for international cooperation within multinational bodies such as UNCTAD, WTO, the European Union, OECD, APEC and others. Stephen Lau, Hong Kong's Privacy Commissioner, has drawn attention to the high level of concern reported amongst computer users and net users in 1998 both about the privacy and security of their personal data.[35] He has mentioned the demands of consumers and their representatives to be informed of the providers' policy on data privacy; to have a choice of anonymity for browsing and transacting business; and to be able to ensure encryption facilities for the collection and use of sensitive data. One suggestion in this context is accreditation of information systems with a recognised 'privacy seal'. This would provide effective assurance to consumers on the suppliers' compliance with an adequate privacy policy.[36] We can be sure that governments would want to crack such seals where they consider this to be warranted for law enforcement, intellectual property protection and taxation objectives.

Genetic Privacy

One of the most dynamic technological changes occurring today involves the marriage of information technology and human genetics. Scientists collaborating in the Human Genome Project are in the process of sequencing the entire genome and thereby discovering the keys that will unlock what have hitherto been the mysteries of the basic building blocks of life in the human and other species.

In future it will be possible to analyse the DNA of every individual and to gain a remarkably detailed map of that individual's genetic predispositions and likely health. It may be anticipated that, unless restrained by law, governments, employers, insurers and others may, in some circumstances, seek access to data of this kind. Already in Australia a Genetic Privacy and Non-Discrimination Bill 1998 (Cth) has been introduced as a Private Member's measure.[37] Because of the implications raised for genetic privacy and discrimination, a Senate Committee has recommended that the Bill be considered by a national working party. The primary purposes of the Bill are to establish an enforceable right to privacy of genetic information of an individual; to prevent any person collecting a DNA sample from the individual without informed consent and to make discrimination based on genetic information unlawful.

Concerns of this kind were simply not around when the OECD Expert Group delivered its report in 1980. Many of them did not exist when the OECD report on Security of Information Systems was delivered in 1992. Doubtless further and more complex developments will occur between now and the end of the next 20 years. What may be needed is an ongoing institutional arrangement by which the advances of technology and their implications for the OECD Guidelines on Privacy can be kept under constant review.

State of Privacy

Also needed is a regular and universally respected report on the state of privacy which is increasingly rendered vulnerable by the remarkable developments of technology. A recent review of Asian privacy and surveillance laws[38] found most of them inadequate. In the case of Hong Kong, the review criticised as unacceptably vague the procedural safeguards on the interception of telecommunications permitted by law.[39] In India, there is no privacy or data protection statute, and illegal wire-tapping by governmental agencies was said to be continuing.[40] In Japan, although legislation governing the use of personal information in computerised files held by government agencies was adopted in 1988, in line with the OECD Guidelines, the private sector is still substantially unregulated. Various complaints have been made concerning police video surveillance systems. The Republic of Korea, like Japan, has adopted legislation drawn from the OECD Privacy Guidelines[41] for the protection of personal information in public computer-based information systems. Credit reports are regulated by statute in Korea, but there has been criticism of the lack of effective accountability of intelligence and police officials using electronic interception. In most other countries of Asia, removed from the stimulus and impetus of the OECD, the law is in an even more primitive and unprotective state.

It is therefore timely that we should be reconsidering privacy protection and doing so in a global and regional context, not one confined to the cosy club of like thinking western countries. Privacy is a universal value, as the instruments of the United Nations declare. It is not a culture-bound value only relevant to advanced Western democracies. Whilst the exact content and priorities for privacy protection will differ from one country

to another and will vary as between different cultures, the core value is the same. It inheres in the dignity of each individual human being. It gathers universal significance because of the dynamic forces of global technology: the Internet, global e-commerce and the Human Genome Project.[42]

A New Beginning?

In 1980, a small band of intrepid individuals in a trans-continental organisation representing different cultures amongst the rich countries of the world laid down a framework of privacy principles which has been extraordinarily successful and remarkably enduring: but that was the old testament. So dynamic have been the changes of technology in the interim that a new testament is now needed. It will embrace the outcomes of technological advances and recognise that they are overwhelmingly to the benefit of humanity. It will also demand that they go forward with a social and legal regime that upholds and protects the individual's right to privacy and to data protection and data security.

From humble beginnings much has been accomplished. The achievement of 1980 shows that international consensus can indeed be found and can be extremely useful, but it would certainly be remarkable if the words written in 1980 were to be the last expression of the international principles for personal privacy and data protection. They are not writ in stone. They exist in disembodied electronic form as befits our age of revolutionary technology. Using them, we should chart the way ahead for privacy protection for Asia and for the world.

According to The *Economist* it is too late. The editor says that we cannot even restore the levels of privacy enjoyed in the 1970s. Most people, he asserts, do not care. With greater surveillance comes the chance of greater safety in shopping malls and urban streets. A universal data bank of DNA will allow criminals to be found and convicted. International satellite monitoring of telecommunications by *Echelon* will make the world safer from terrorists. The *Economist's* conclusion: 'The best advice is: get used to it'.[43]

But not everyone takes this attitude. The European Union's *Data Protection Directive* is striving to defend privacy values. Not many jurisdictions of the world outside Europe meet the Directive's demand that the laws of other places, sharing personal data with European systems, must 'effectively' protect personal data. Already this has led to negotiations with a view to providing more effective privacy laws.[44] The Australian Government, after initially promising privacy protection laws applicable to the private sector and then resiling, has now returned to its original intention and new legislation is awaited.

There are two visions for the future here. One defends individual privacy; the other gives up. One asserts the capacity of law and policy-makers to uphold a fundamental human right in the face of technology; the other says it is impossible—and possibly unnecessary. Resolving these debates presents one of the greatest questions before humanity in the coming century. The resolution will shape the human environment and all that follows. What is at stake is nothing less than the future of the human condition.

Notes and References

1. A paper presented at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September 1999.
2. Organisation for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, 1981.

3. The history is told in Australian Law Reform Commission, *Privacy*, Report No. 22, Vol. 1, 1983, 264 ff.
4. Council of Europe, *Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data* (adopted September 1980).
5. *Universal Declaration of Human Rights* (1948) Article 12; *International Covenant on Civil and Political Rights* Article 17.
6. *European Convention of Human Rights*, Article 8. *American Declaration of Rights and Duties of Man* (1948) Article V. *American Convention on Human Rights* (1969) Article V. cf L. Bygrave, 'Data protection pursuant to the right to privacy in human rights treaties', *International Journal of Law and Information Technology*, 6, 1998, p. 247.
7. *Dudgeon v United Kingdom* (1981) 4 EHRR 149.
8. *Norris v Republic of Ireland* (1988) 13 EHRR 186.
9. *Modinos v Cyprus* (1993) 16 EHRR 485.
10. *Toonen v Australia* (1994) 1 *Int Hum Rts Reports* 97, extracted in H. J. Steiner and P. Alston, *International Human Rights in Context*, Oxford, 1996, p. 545. The decision led to the enactment by the Australian Federal Parliament of the *Human Rights (Sexual Conduct) Act* 1994 (Cth) and subsequently to the repeal of ss 122(a) and (c) and 123 of the *Criminal Code* (Tas) by the Tasmanian Parliament and the adoption of reformed non-discriminatory offences.
11. *Privacy Act* 1988 (Aust).
12. *Privacy Act* 1993 (NZ). The Act did not fully commence in operation until July 1996.
13. T. McBride, 'The review process—taking on the critics', *PLPR*, 5, 1998, 6 at 101.
14. B. Stevens, 'The review's treatment of the information privacy principles', *PLPR*, 5, 1998, 6 at 120.
15. 'From barriers to solutions: the OECD Ministerial on electronic commerce' [4th Quarter 1998] *I-Ways*, p. 38.
16. *Ibid.*
17. *Ibid*, p. 46.
18. *Ibid.*
19. OECD Ministerial Declaration on Privacy on Global Networks [4th Quarter, 1998] *I-Ways*, p. 48.
20. The entire text of the Ministerial Declaration can be found at http://www.otawaoecdconference.org/
21. See 'The end of privacy', *The Economist*, 1 May 1999, p. 11 and 'The surveillance society', *The* Economist, 1 May 1999, pp. 17–19.
22. R. Miller, *The Internet in Twenty Years: Cyberspace, the New Frontier?* OECD, Paris, 1997. Cf M. D. Kirby, 'Privacy in cyberspace', UNSW *Law Journal*, 21, 1998, p. 323.
23. W. Gibson, *Neuromancer*, cited in M. S. Borella, 'Computer privacy versus first and fourth amendment rights', http://www.eff.org/pub/Privacy/compprivacy4thamend.paper,cf E. France, 'Can data protection survive in cyberspace?', *Computers and Law*, 8, 2, 1997, p. 20.
24. Miller, *op. cit.*
25. E. Cornish, 'The cyber future: 92 ways our lives will change by the year 2025', *The Futurist*, 30, 1, 1996, p. 27, abstracted in OECD, *op. cit.*, at p. 12.
26. G. Greenleaf, 'Privacy in cyberspace: an ambiguous relationship, *PLPR*, 3, 1996, 5 at 88.
27. S. D. Balz and O. Hance, 'Privacy and the Internet: intrusion, surveillance and personal data', *International Review of Law, Computers and Technology*, 10, 2, 1996, p. 219.
28. Greenleaf, *op. cit.* A catalogue of Internet privacy issues may be found at: http://www.anu.edu.au/people/Roger. Clarke/DV/Internet.html
29. See http://www.altavista.digital.com
30. J. Hilvert, in *Information Age*, May 1996, pp. 18–23, cited by Greenleaf, *op. cit.*, at 89–90.
31. Organisation for Economic Cooperation and Development, *Guidelines for Cryptography Policy*, 27 March 1997 (OECD.doc.C (1997) 62/Final). Cf J. Adams, 'Encryption: the next best thing?', *Computers and Law*, 2, 1998, 39 at 40.
32. G. Greenleaf, 'Privacy principles—irrelevant to cyberspace?', *PLPR*, 3, 1996, 6 at 114, 118.
33. R. Clarke, 'Profiling and its privacy implications', *PLPR*, 1, 1994, 7 at 128–129; R. Wacks, 'Privacy in cyberspace: personal information, free speech and the Internet', in P. Birks (ed.), *Privacy and Loyalty*, Oxford, 1997, at 93.

34. H. H. Perritt and C. J. Lhulier, 'Information access rights based on international human rights law', *Buffalo Law* Review, 45, 1997, 899 at 906 ff.
35. S. Lau, 'E-commerce, consumer rights and data privacy' [3rd Quarter, 1998], *I-Ways*, p. 37.
36. *Ibid*, p. 38.
37. Australia, Senate Legal and Constitutional Legislation Committee, Consideration of Provisions of the Genetic Privacy and Non-Discrimination Bill 1998 (March 1999).
38. D. Banisar and S. Davies, 'CILC's survey of Asian privacy and surveillance laws', *PLPR*, 5, 1998, 5 at 86.
39. *Telecommunications Ordinance and Post Office Ordinance*.
40. Banisar and Davies, *op. cit.* at 87.
41. *Ibid*, at 88.
42. Cf J. Hagel and M. Singer, 'Private lives—electronic commerce', in *The McKinsey Quarterly*, 1, 1999, p. 7.
43. *The Economist*, May 1999, p. 12.
44. The revised Safe Harbor Privacy Principles, published 19 April 1999, may be seen at www.ita.doc.gov/ecom/shprin.html