1519

UNIVERSITY OF NEW SOUTH WALES LAW JOURNAL

PRIVACY IN CYBERSPACE

The Hon Justice Michael Kirby AC CMG

UNIVERSITY OF NEW SOUTH WALES LAW JOURNAL

PRIVACY IN CYBERSPACE*

The Hon Justice Michael Kirby AC CMG**

A NEW DYNAMIC

Time passes. Twenty years ago in the Organisation for Economic Co-operation and Development (OECD) work was beginning towards guidelines on the protection of privacy in the context of trans-border data flows[1]. Ten years ago work towards the later OECD guidelines on security of information systems was commenced[2]. I chaired the two expert groups which prepared those

---

* This is an abbreviated and amended version of a paper to be published in *International Dimensions of Cyberspace Law* by the United Nations Educational, Scientific and Cultural Organisation (UNESCO), Paris in 1999.

** Justice of the High Court of Australia. Lately President of the International Commission of Jurists. One-time Chairman of the OECD Expert Groups on Privacy (1978-1980) and Data Security (1991-1992).

1 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Paris, 1980.

2 OECD, *Guidelines on Security of Information Systems,* Paris, 1992.

successive principles. That work opened my eyes to the enormous implications of modern technology for the law and human rights in every society. And to the capacity of international institutions to help municipal law-makers respond to global problems. The work of the OECD on the social and legal issues presented by informatics illustrates the way in which the international community is slowly but inexorably constructing a mutually compatible legal order on the foundation of "respect for human rights and fundamental freedoms"[3].

Ten years ago, I suggested[4] that what was lacking at the international level, as in domestic jurisdiction, was a perception of the relevance of scientific developments for the *concept* of human rights. This was because of the fragmentation of priorities, the dominance in the debates on human rights of lawyers (often ignorant of science), the limited perspective of specialised institutions and the highly controversial nature of many of the moral dilemmas posed. It is useful, I think, to repeat my conclusion[5]:

---

3 Preamble to the Charter of the United Nations. See L M Gruderidge and E Hambro, *Charter of the United Nations: Commentary and Documents,* second ed (1949), 87.

4 M D Kirby, "Human Rights and Technology: A New Dilemma" (1988) 22 *Uni British Columbia Law Review* 123 at 127.

5 *Ibid,* 130-131. Cf A E S Tay, *Teaching Human Rights,* Aust National Commission for UNESCO, 1981 at p 2.

> "... [T] here has been little endeavour to reflect the major scientific and technological developments of the last fifty years, and their impact on human rights, in a conceptual way. Instead, old human rights instruments developed for earlier times are scrutinised for their possible utility in solving the controversies presented by the new technology. Piece-meal legislation is enacted. No Luther of jurisprudence has emerged to pull together the implications of nuclear physics, informatics and biotechnology for 21st century man and woman."

In the decade since those words were written, the fundamental problem remains unresolved. The urgency of finding solutions has increased. In informatics, there has been a rapid convergence of technologies. Telecommunications have merged with computerisation linked with other systems of communication[6]. Connections have been forged between nuclear physics, informatics and biotechnology. The *Star Wars* system proposed by President Ronald Reagan had a worrying potential to link nuclear weaponry and informatics. The Human Genome Project would not be possible but for the linkages of information technology and biological research[7]. It is important to realise the interconnections of scientific advances and to study their impact on human rights. For example,

---

6 J Bond "Telecommunications is Dead, Long Live Networking" in *I-Ways*, Third Quarter 1997, at p 26.

7 R Cook-Deegan, *The Gene Wars,* Norton, New York, 1994, 283ff; M D Kirby, "The Human Genome Project - Promise and Problems' in 11 *Journal of Contemporary Health Law and Policy* 1 (1994). See now UNESCO, *Universal Declaration on the Human Genome and Human Rights* (1997) esp articles 7, 8 and 9.

the privacy of genetic information is as much an issue for human rights in the context of informatics as it is in the context of biotechnology. Principled responses, defensive of the rule of law, human rights and fundamental freedoms, will necessarily have common themes.

In the twenty years since the OECD Guidelines on Privacy were formulated, the Internet has been launched. It expands at an astonishing rate with world-wide users doubling every twelve months[8]. William Gibson's vision of cyberspace[9] is fast becoming a reality. Starting with 8.5 million users in 1995, the Internet is expected to reach over 142 million users by the year 2000[10]. For a pertinent analogy, it is necessary to go back to Gutenberg's printing press[11].

---

8 R Miller in OECD Future Studies Information Base Highlight, No 14, May 1997: *The Internet in Twenty Years: Cyberspace, the Next Frontier*?, OECD, Paris, 1997 at p 1.

9 Gibson, W, *Neuromancer,* cited M S Borella, "Computer Privacy vs. First and Fourth Amendment Rights" (http://www.eff.org/pub/privacy/comp privacy fourth amend appear). As Miller notes (above n) cyberspace will eventually come to life on the Internet infrastructure as a range of information and services spanning, at least for a few analysts, almost all aspects of human experience. Cf E France, "Can Data Protection Survive in Cyberspace?" (1997) *Computers and Law* at 20.

10 Miller, above n 8.

11 Five hundred years ago Francis Bacon, writing about Gutenberg's printing press, commented on how the very way humans thinking would be rearranged, changed and as he put it

Footnote continues

Look ahead. Imagine the way in which, in the future, the lives of human beings will be altered as the global network of inter-connected users of information technology becomes bigger and even more powerful. Already, informed writers are offering their predictions. Edward Cornish, for example[12], has sketched ninety-two ways in which, he claims, the lives of ordinary people will change over the next thirty years as a result of the Internet. Global culture, education, employment, production and even crime will be affected. Local cultures and languages may decline. Increased drug use and the risks of cyber-crime and terrorism will be larger problems. Privacy, it is argued, will be harder to maintain. Not unconnected with this, inter-personal relationships of human beings will be increasingly unstable. Cornish's conclusion is that the unprecedented power to choose will often result in less sensible action and greater conflict. Governments will have limited control over cyberspace and over the pace at which globalisation of the inter-connected human consciousness is occurring.

"the appearance and state of the world" would be altered. Cf S Harris cited in S Williamson, "Legal-Holes in the Information Super Highway", Victoria, *Law Institute Journal,* 1995 at p 1213.

12 "The Cyber Future: 92 Ways our Lives will Change by the Year 2025" in *The Futurist,* Vol 30 No 1 pp 27-42 (1996) abstracted in OECD, above n 8, at p 12.

ENDANGERED PRIVACY

Many of the problems for privacy which were identified in the 1980s are now enlarged, or altered, by the development of the Internet. The speed, power, accessibility and storage capacity for personal information identifying an individual are now greatly increased[13]. Some of the chief protections for privacy in the past arose from the sheer costs of retrieving personal information; the impermanency of the forms in which that information was stored; and the inconvenience experienced in procuring access (assuming that its existence was known). Other protections for privacy arose from the incompatibility of collections with available indexes and the effective undiscoverability of most personal data. These practical safeguards for privacy largely disappear in the digital age[14]. A vast amount of data, identified to a particular individual, can now be collated by the determined investigator. The individual then assumes a virtual existence which lives in cyberspace instead of in what is sometimes described as "meat space"[15]. The individual takes on a

---

13 A Cavoukian and D Tapscott, *Who Knows - Safeguarding your Privacy in a Networked World,* Vintage, Canada, 1996; S D Balz, and O Hance, "Privacy and the Internet: Intrusion, Surveillance and Personal Data" (1996) 10 *International Review of Law, Computers and Technology* No 2, at p 219.

14 G Greenleaf, "Privacy and Cyberspace - An Ambiguous Relationship" in *Privacy Law and Policy Reporter* Vol 3 #5, August 1996 at p 88.

15 *Ibid,* at p 89.

digital persona made up of a collection of otherwise unconnected and previously unconnectable data.

This quantity of personal information about individuals is likely to increase rather than decrease[16]. Access to this information is what occasions the contemporary fragility of privacy - a human attribute that has been steadily eroded over the past century[17]. To the extent that the individual has no control over, and perhaps no knowledge about, the mass of identifiable data which may be accumulated concerning him or her and to the extent that national law-makers, despite their best endeavours, enjoy only limited power effectively to protect the individual in the global web, privacy as a human right, is steadily being undermined[18].

It is not always appreciated by users of the web that without specific initiatives on their own part, their visits to particular websites can usually be resurrected: presenting a profile of their minds. These visits may illustrate the subjects in which they are interested:

---

16 *Ibid*, at p 88.

17 R Wacks, "Privacy in Cyberspace: Personal Information, Free Speech and the Internet" in P Birks (ed) *Privacy and Loyalty*, Oxford 1997 at p 93.

18 Wacks, above n.17, at p 110; Balz and Hance, above n 13, at p 220.

their inclinations, political, social, sexual and otherwise[19]. An early indication of the potential of this form of surveillance to pry on the individual occurred during the confirmation hearings in the United States Senate considering the nomination of Judge Robert Bork to the United States Supreme Court. A reporter retrieved the record of Judge Bork's video rentals as itemised by computer[20]. Nor is this a theoretical danger. Senior Petty Officer Timothy McVeigh, a naval officer stationed in Hawaii, was discharged from the United States Navy after he came under investigation following the search of his America On Line ("AOL") profile which included the word "gay". An acquaintance turned the profile over to Mr McVeigh's command. It treated it as a breach of the United States government's policy about the sexual orientation of service personnel, described as "Don't ask. Don't tell". Mr McVeigh did not tell: but AOL did[21].

One of the particular dangers of data profiling is the human tendency to assume that because information comes out of an

---

19 Balz and Hance, above n 13, at p 222. Most Internet users do not seem to appreciate that an image of a site they may have visited many weeks earlier could be stored in their personal computer and easily viewed by another person having access to the computer.

20 *Ibid*, at p 228.

21 Human Rights Campaign: "Human Rights Campaign Learns Pentagon Postponing Expulsion of Sailor with "Gay" in is Profile" (http://www.hrc.org/feature.1/mcveigh.html). A judge has granted temporary relief to Mr McVeigh against dismissal.

automated system, it must be accurate. Data profiles have a potential to magnify and endlessly to reproduce human error[22]. There are many studies of the mistakes which can occur. The brother who once paid a defaulting sibling's rent and found himself black-listed as an unreliable tenant. The network user whose facilities are used by someone else to make a visit to a child pornography website or to download child pornography whilst the user is away.

The damage that can be done through defamation on the Internet is illustrated by a recent case in Western Australia. A message from an anthropologist appeared on the World Wide Computer Network Bulletin Board defending a university decision not to grant academic tenure to the plaintiff. The message mentioned an accusation of sexual misconduct which thereupon became available to approximately 23,000 academics and students, within the relevant speciality, having regular access to the bulletin board. Defamation was found and damages awarded[23].

---

22 T Miller, "Law, Privacy and Cyberspace" (1996) 1 *Communications Law* No 4 p 143 at p 145; H Wright, "Law, Convergence and Communicative Values on the Net" in (1996) 7 *Jl of Law and Info Science* 54 at 65..

23 *Rhindos v Hardwick*, unreported, Supreme Court of Western Australia, (Ipp J), 31 March 1994 noted in G Hughes, "Nowhere to Hide? Privacy and the Internet" (1996) 29 *Computers and the Law* 21 at p 22; B Todd,, "From Village Pump to Superhighway: Internet and the Modern Law of Defamation" (1996) 1 *Media and*

Footnote continues

It is not accurate to say that the Internet is a law-free zone. Much local law applies to the activities occurring there. But it is true to say that there is no global authority which controls the Internet. There is no uniform global regime to regulate and enforce standards[24]. To some extent the absence of a controlling and enforceable law facilitates free expression, the communication of ideas and notions of individual liberty which are themselves important human rights. However, such values are not the only human rights, as a glance at the *Universal Declaration* and its progeny of international law will demonstrate. There are other fundamental human rights which sometimes compete, or conflict, with the right of free expression. The right to privacy and to reputation and honour, and the confidentiality of communications must also be protected[25]. In the world of the Internet, technological capacity tends to favour the spread of information. The protection of competing values is decidedly weak.

Arts Law Review (Aust), 34; P Bartlett, "Internet & the legal tangle" (1995) 1(4) *Computer Law and Practice* 110.

24 Miller, above n 8, at p 145.

25 *Universal Declaration of Human Rights,* Article 12; *International Covenant on Civil and Political Rights,* Article 17.1. See generally H H Perritt and C J Lhulier, "Information Access Rights Based on International Human Rights Law", 45 *Buffalo Law Review* 899 at 906ff (1997).

With the Internet have come additional problems. Because of the growing use of information systems by business and government, and because these are connected to the Internet, many transactions by individuals in every country will now be potentially inter-connected and examinable. This will afford means of distributing data about the individual to remote places and, often, to persons or organisations with which the individual may have no other connection. The advent of search engines, robots, wanderers and Internet indexes present a new dimension to the isolation of personally identifiable data profiles. The extensive indexes of Internet sites such as *Yahoo*[26] and the launch in December 1995 of the *Altavista* search engine[27] (with the subsequent proliferation of e-mail, telephone, address and Usenet directories) change forever the personal profile potential of the individual. In his essay "Private Lies"[28], John Hilvert describes *Altavista* in these terms:

> "[It] was introduced as a free service back in December [1995] to show [Digital Equipment Corporation's] ability to handle the Internet, no matter how it scaled. ... [It] gobbles and disgorges in a very accessible way the entire catalogue of some 22 million web pages (12 billion words) and about two months of the content of

---

26. Greenleaf, above n 14, at p 88. A catalogue of Internet privacy issues may be found at http://www.anu.edu.au/people/Roger.Clarke/DV/Internet.html.

27. http://www.altavista.digital.com.

28. In *Information Age,* May 1996, pp 18-23 cited Greenleaf above n 14 at pp 89-90.

> 15,000 news groups. It handles 5 million search requests a day. Impressed with *Altavista's* remarkable speed. [The subject tried *Altavista* on the news groups and was sickened. 'What I found ... using my name or e-mail address as search parameters, was a copy of almost every post I've made to Newsnet news groups since the first week in January. ... That includes my posts to these two news groups, and all rejoinders from anyone here who included my name in his or her reply. Make out of that what you wish. My reaction to it is somewhere between disgust and fury. 'What I do not expect is that the news group clubhouse is bugged and that what is said there, by any of us, will be recorded and made available to any person on the Internet, for whatever reason persons might have'. The irony of this is: I came across [this] ... using the *Altavista* search engine."

Users commonly think that, because they do not enter their names or other details to gain access to web pages, this means that there is a high degree of privacy in their use of the Internet, ie that it is virtually anonymous. However with most web browsing software, such as Netscape and Microsoft Explorer, any request to a web site discloses the network identity of the machine used to access the web, the web page immediately previously accessed, together with related "cookies", such as information stored by the web server on the computers of users who have accessed it, the list of previously accessed web pages or transactional information generated while accessing those web pages[29]. If this does not cause anxiety about the potential loss of privacy of Internet users, nothing will.

---

29 *Ibid,* pp 91-92. Without spiders and robots it would be very difficult to find information on the web. These "devices" continually travel the millions of Internet servers on the web and index every significant word or phrase on each one. Web

Footnote continues

Of course, this is not a reason, Canute like, to hold up the hand against progress. On current trends we can scarcely prevent the rapid continuing growth in Internet users. Nor would one wish to do so. But it does present a challenge to those who would defend fundamental human rights (including privacy) and those who realise that false, distorted, damaging, hurtful and intrusive information that can be compiled about an individual based upon data received from a multitude of digital sources and given an apparent authenticity by digital delivery. Web crawlers, spiders, robots and trawlers introduce a new dimension to the info-privacy debate. They also challenge the applicability, in today's technology, of some of the OECD Guidelines prepared in the context of the technology of earlier decades, when such intense dataveillance was not foreseen[30].

CHALLENGES TO DEMOCRATIC GOVERNANCE

In addition to the foregoing concerns an even deeper malaise must be addressed. It relates to the capacity of presently existing

---

"masters" can prevent their sites from being so indexed. The awareness of the danger and the ways of meeting it has heightened in recent times. In 1994, an attempt was made to draft a *Robot Exclusion Standard.* See http://web.nexor.co.uk/mak/doc/robots/norobots.html.

30 R Clarke, "Profiling and its Privacy Implications" *Privacy Law and Policy Reporter,* vol 1 #7, pp 128-129, Wacks, above n 17, at pp 93-97.

lawmaking institutions to respond adequately to the problems which the new technology presents. Privacy is only one attribute of the Internet in which challenges arise for established values. Organised crime, terrorism, infringement of intellectual property rights, unconsensual or under-age infiltration of pornography are some of the other problems examined in the literature[31]. So are the implications of the Internet for the integrity of financial markets, for tax avoidance and tax havens[32]. Equally controversial is the impact of the Internet upon cultural sovereignty and diversity[33] which is of such concern to societies struggling to preserve and defend their language, religious or spiritual values, moral norms and distinct social diversity.

In striking down the censorship provisions of the *Communications Decency Act* of the United States[34], the Supreme Court of that country itself recognised, that the practical consequence

---

31 C Downey, "The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?" 14(2) *John Marshall Journal of Computer and Information Law* at p 303 (1996).

32 Wacks, above n 17 at p 111.

33 S Davies, "Strategies for Protecting Privacy in the New Information Structure" in *Privacy Law and Policy Reporter* Vol 2 #2, 1995 at p 23; cf *I-Ways*, Fourth Quarter, 1997 at p 9.

34 *Reno v American Civil Liberties Union,* 138 L Ed 2d 574 (1997) noted *Computer Law and Security Report* Vol 13 No 5 1997 at p 371.

of its decision would reach far beyond the borders of the United States of America[35]:

> "Once the provider posted its content on the Internet it could not prevent that content from entering any community. Thus, 'when the UCR / California Museum of Photography posts to its website nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit would travel to Baltimore and New York City those images are available not only in Los Angeles, Baltimore and New York City but also in Cincinnati, Mobile or Beijing - wherever Internet users live. Similarly, the safe sex instructions that 'Critical Path' posts to its Web site written in street language so that the teenager receiver can understand them, are available not just in Philadelphia, but also in Provo and Prague".

People in every country are therefore, in a sense, beneficiaries of decisions made upon the First Amendment to the United States Constitution. Not all societies, and certainly not all governments, necessarily share the social values reflected in the United States court decisions. In a number of countries attempts have already been made by law to control the Internet[36]. Thus a draft law in Thailand purports to prohibit dissemination through the Internet of information that is against "public peace and order and may lead to disunity of the nation or deterioration of international relationships"; "immoral information"; "information disparaging religion" or "highly

---

35 *Reno, ibid,* at p 372.

36 China, Singapore and Germany have introduced laws. See Wacks, above n 17, at p 99.

respected persons" and "inappropriate information" concerning the King of Thailand, the Thai Royal Family and also "Heads of State of friendly foreign countries"[37]. This law was roundly criticised when it was published in January 1998, on the ground the last-mentioned provision would create criminal offences for disseminating sexual information concerning President Clinton of the United States. The subsequent publicity given to allegations against the President, and its dominance of much of the global news media, demonstrated once again the difficulty (and possibly undesirability) of censoring the international flow of data of this kind.

Another illustration lies in the efforts of the British Government to prohibit publication of information and commentary which might endanger the fair trial of Mrs Rosemary West. She was accused of involvement in notorious serial killings. Such efforts of control might have been effective in the traditional news media. But they were wholly ineffective in the Internet[38]. The earlier attempts of the British Government to suppress the publication of the book *Spycatcher* by Mr Peter Wright failed in the courts of several countries outside the

---

37 Internet Promotion Bill 1998 (Thailand) (Draft 4) noted *Bangkok Post,* 12 January 1998 at pp 1-2.

38 T Miller, "Law, Privacy and Cyberspace" (1996) 1 (4) *Communications Law* 143 at p 145.

United Kingdom[39]. It was not even attempted in the United States of America. The case illustrated the effective powerlessness of most national courts to enforce, in a truly effective way, local norms and values affecting global information.

Governments and legislatures are not wholly powerless in the face of the Internet and global media. But the force of the technology (and the vast audiences which it gathers up) suggest that common global standards will tend, in time, to swamp local susceptibilities. At least in the case of most countries, there will be little which they can do to influence the information flow except to enact laws enforceable in their courts in the comparatively rare instances in which they can catch those who offend against such laws within their jurisdiction.

Some will say that this limitation on the incapacity of national law-makers to respond to the challenge of the Internet is nothing but an illustration of globalisation which technology more generally renders irreversible and inevitable. The contribution of the Internet to free expression, democratic practice and individual liberty cannot be denied. But in the interval between the receding power of national law and the lack of effective international law, lie certain dangers. As I have shown, they are dangers for those human rights which

---

39 See eg *Attorney General (UK) v Heinemann Publishers Australia Pty Ltd* (1988) 165 CLR 30.

compete with the free flow of undigested data. They are also dangers to stable social regulation on the part of those who see the impact of the new values which multimedia and the Internet bring and object to aspects of what they see.

AN AGENDA FOR ACTION

The result of this review is that the extraordinary development of informatics continues to present puzzles and challenges both to the international community and to the law-making institutions of the nation states which make it up. A number of things can be done:

1. Every jurisdiction needs to review its applicable laws and policies to adapt them to the new technology. In the United States a constitutional amendment has even been proposed to update some of the present legal guarantees and to permit courts to fashion new principles in harmony with the new technology and new values[40]. In Australia, in the space of a year or two, three discussion papers have been produced by official bodies. There is currently a Senate inquiry on self-regulation in the information and communications industries[41].

---

40 See Professor Laurence Tribe's suggestion noted Wacks, above n 17, at p 99.

41 The three initiatives of the Australian Government are explained in T Hughes, "Regulation of the 'Net'" in Australian Law Reform

Footnote continues

It is highly desirable that in every jurisdiction legislators, governments, academics and the community generally should be debating the social implications of the new technology, including the Internet. Such debates need to be supplemented by international initiatives which seek to devise principles as global as the technology itself. Otherwise, we will persist with a legal patchwork of dubious effectiveness[42] and more and more business and other communications will take place in extra - and supra - jurisdictional space.

2. The development of "cyber manners", of Internet standards and the initiatives of bodies such as the Global Internet Liberty

---

Commission, *Reform* Issue 71, 1997, 23 at 24. They concern privacy protection, copyright reform and the regulatory framework of online services. Subsequently the Australian Government withdrew an electoral commitment to enact privacy legislation for the private sector. See S Davies, "Privacy Law - Australia" in *Computer Law and Security Report,* Vol 16 No 6 (1997), 429. The Government of Victoria has announced that it is drafting legislation to place all legislation on line. See *Australian Financial Review,* 24 October 1997 at 27. At the time of writing the Australian Senate Select Committee on Information Technology is conducting an inquiry on self-regulation in the information and communications industries.

42 Greenleaf, "Privacy Principles - Irrelevant to Cyberspace?", *Privacy Law and Policy Reporter* Vol 3 No 6 (1966) at 114 at pp 118-119. The European Union has proposed a process that could lead to an "International Communications Charter" by the end of 1999. See *I-Ways,* First Quarter 1998 and <eif@bxl.dg13.cec.be>.

Campaign[43], as well as domestic initiatives to advocate endangered rights such as privacy[44], deserve support.

3. There is an urgent need, in the light of technological change and the enhanced capacity of the Internet, for a review to be conducted of the information privacy principles developed by the OECD twenty years ago. There are serious gaps in those principles. Informed writers are already suggesting that new privacy principles are needed, such as:

* A right not to be indexed - if a "rogue" robot indexer ignores existing or new contemporary standards which exclude indexing.

* A right to encrypt personal communications effectively[45].

---

43 *Ibid,* at p 119.

44 The Australian Privacy Charter Council is a non-governmental organisation established to promote the protection of privacy. It has issued a Privacy Charter. See (1995) 2 *Privacy Law and Policy Reporter* 44. See also the European Union's *Data Directive* (Directive 95/46/EC. Cf G Greenleaf, "European Commission tests adequacy of our privacy laws" in *Privacy Law and Policy Reporter,* Vol 4 #8 January 1998 at p 140 and S Lau, "Observance of the OECD Guidelines and the EU Directive in Asia" in *Privacy Law and Policy Reporter,* vol 4 #8 at p 145.

45 See OECD, *Guidelines for Cryptography Policy,* 27 March 1997 which include a set of eight principles relevant to this discussion. Principle 2 relates to users' rights to choose cryptographic methods. Principle 5 relates to the individual's rights to privacy including secrecy of communications and protection of personal

Footnote continues

* A right to fair treatment in public key infrastructures, so that no person is unfairly excluded in a way that would prejudice that person's ability to protect their privacy.

* A right to human checking of adverse automated decisions and a right to understand such decisions[46].

* A right, going beyond the aspiration of the OECD 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[47].

4. A common theme of many of the proposed revisions of the OECD Privacy 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 made known prior to operation and ...

---

data. OECD Doc:C(97) 62/FINAL. Cf J Adams, "Encryption - The Next Big Thing?" *Computers and Law,* Feb 1998, 39-40.

46 G Greenleaf, "Privacy Principles - Irrelevant to Cyberspace?", *Privacy Law and Policy Reporter,* Vol 3 #6 (1996) 114 at 118.

47 Clarke, above n 30, at p 129. See also R Clarke, "Beyond 'Fair Information Practices': A new Paradigm for 21st Century Privacy Protection" at http://www.anu.edu.au/people/Roger.Clarke IDV/Beyond FIP.html.

the individual should retain the ability to disengage the feature if he or she so chooses"[48]. Whilst some observers would contest such an absolute statement of the right of disengagement (and whilst others might question the marginal utility of undemanded notification of all identifiable information about an individual without any initiative on the part of that individual) clearly the openness principle of the OECD Guidelines is one of the weakest in the collection. The advent and potential of the Internet requires that there be new attention to it[49].

5 The role of national governments as the defenders of privacy and of fundamental rights also needs careful consideration, given the past record of many of such governments as intruders into such fundamental rights. This, together with commercial concerns, provides the explanation for the strong resistance to the Clipper Chip proposed by the United States Government in 1993. That proposal had the ostensible

---

48 H H Perritt and C J Lhulier, above n 25. See also G Greenleaf, above n 14, at p 92. cf M Rotenberg, "Privacy and Protection - A US Perspective: Data Protection in the United States - A Rising Tide?" in *Computer Law and Security Report* Vol 14 No 1 1998 at pp 38-40.

49 Davies, above n 33, at p 38. The Australian Privacy Commissioner has issued new *National Principles for the Fair Handling of Personal Information* which include an anonymity principle.

purpose of allowing government to override individual encryption, allegedly to protect society from "gangsters, terrorists and drug-users"[50]. The first two words are loaded. The third, at least now, engenders a legitimate international debate concerning the proper global strategy to respond effectively to the drug epidemic. Whilst society needs to be shielded from clearly antisocial conduct, there are strong arguments for permitting, and protecting, the anonymity of most website visits[51] and providing "dungeons" and "chat rooms" in the web where people can communicate without fear that their interests, attitudes, beliefs and concerns will be monitored either by the public or the private sectors[52].

6. One feature of Internet reporting is the intensification of the competition for getting the "news" first. This puts great pressure upon modern journalistic standards. The kind of reporting which has lately affected public personalities such as Diana, Princess of Wales, and President Clinton, in respect of their private lives is, in part, a product of the new technology. No public figure is entitled to protection in relation to aspects

---

50. Wacks, above n 17, at p 107.

51. *Ibid,* at p 100.

52. *Ibid,* at p 98.

of private life which may have relevance to public duties. But unless public figures can enjoy a private zone where their lawful family, sexual, health and other data belongs to *them* and is respected by others, the result will be a serious erosion of the quality of persons offering to serve.

A second generation of information privacy principles, in harmony with the development of the Internet, should therefore be drawn up without delay. The Internet should develop in a way respectful to fundamental human rights and democratic governance. Its expansion should reflect global values and human diversity. This is a mighty challenge. Yet the Internet itself was conceived in the minds of human beings. It should be possible for humanity to devise and apply just rules for its operation[53]. If it cannot, that fact has serious implications for the notion that human rights are universal. It has profound consequences for the future of the rule of law in cyberspace.

---

53 B Phillips (Canadian Federal Privacy Commissioner) cited in E France, "Can data protection survive in Cyberspace?" *Computers & Law,* July 1997, v 8, issue 2, 20 at 24.