INTERNATIONAL COUNCIL FOR COMPUTER COMMUNICATION

ICCC NEWSLETTER

PRIVACY IN CYBERSPACE

The Hon Justice Michael Kirby AC CMG

Governor ICCC

INTERNATIONAL COUNCIL FOR COMPUTER COMMUNICATION

ICCC NEWSLETTER

PRIVACY IN CYBERSPACE*

The Hon Justice Michael Kirby AC CMG**

Governor ICCC

A NEW DYNAMIC

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

---

* 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. In a different form it was published in (1998) 21 *Uni of NSW Law Journal,* 323.

** Justice of the High Court of Australia. Lately President of the International Commission of Jurists (1995-1998). One-time Chairman of the OECD Expert Groups on Privacy (1978-1980) and Data Security (1991-1992). Governor, ICCC.

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

on security of information systems was commenced[2]. I chaired the two expert groups which prepared those successive principles. That work opened my eyes to the 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].

However, 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[4]. Connections have been forged between nuclear physics, informatics and biotechnology. The *Star Wars* system proposed by President Ronald Reagan had a worrying potential to

---

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

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

link nuclear weaponry and informatics. The Human Genome Project would not be possible but for the linkages of information technology and biological research[5]. It is important to realise the interconnections of scientific advances and to study their impact on human rights. For example, 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[6]. William Gibson's vision of cyberspace[7] is fast becoming a

---

5 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.

6 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.

7 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 6) cyberspace will eventually come to life on the Internet infrastructure as a range of information and services spanning almost all aspects of human experience. Cf E France, "Can Data Protection Survive in Cyberspace?" (1997) *Computers and Law* at 20.

reality. Starting with 8.5 million users in 1995, the Internet is expected to reach over 142 million users by the year 2000[8]. For a pertinent analogy, it is necessary to go back to Gutenberg's printing press[9].

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[10]. 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

---

8 Miller, above n 6.

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

10 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.

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[11]. 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"[12]. The individual takes on a 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[13]. Access to this information is what occasions the contemporary fragility of privacy - a human attribute that has been steadily eroded over the past century[14]. 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

---

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

12 *Ibid,* at p 89.

13 *Ibid,* at p 88.

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

effectively to protect the individual in the global web, privacy as a human right, is steadily undermined[15].

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: their inclinations, political, social, sexual and otherwise[16]. 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. The latter 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[17].

---

15 Wacks, above n 14, at p 110.

16 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, 219 at 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 viewed by another person having access to the computer.

17 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 granted temporary relief to Mr McVeigh against dismissal. Subsequently

Footnote continues

One of the particular dangers of data profiling is the human tendency to assume that because information comes out of an automated system it must be accurate. Data profiles have a potential to magnify and to reproduce human error endlessly [18]. 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.

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[19]. 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

---

the dispute was settled and Mr McVeigh was given an honourable discharge. But he was still discharged.

18 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..

19 Miller, above n 6, at p 145.

important human rights. However, such values are not the only human rights. 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[20]. In the world of the Internet, technological capacity tends to favour the spread of information. The protection of values which compete with information flows is decidedly weak.

With the Internet have come additional problems. The advent of search engines, robots, wanderers and Internet indexes presents a new dimension to the isolation of personally identifiable data profiles. The extensive indexes of Internet sites such as *Yahoo*[21] and the launch in December 1995 of the *Altavista* search engine[22] (with the subsequent proliferation of e-mail, telephone, address and Usenet directories) change forever the personal profile potential of

---

20 *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).

21 Greenleaf, above n 11, at p 88. A catalogue of Internet privacy issues may be found at http://www.anu.edu.au/people/Roger.Clarke/DV/Internet.html.

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

the individual. In his essay "Private Lies"[23], John Hilvert describes his first encounter with *Altavista*:

> "[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 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

---

23 In *Information Age,* May 1996, pp 18-23 cited Greenleaf above n 11 at pp 89-90.

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[24]. If this does not cause anxiety about the potential loss of privacy of Internet users, nothing will. 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[25].

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

---

24 *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 "masters" can prevent their sites from being so indexed but few wish to do so and few are bothered. 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.

25 R Clarke, "Profiling and its Privacy Implications" *Privacy Law and Policy Reporter,* vol 1 #7, pp 128-129, Wacks, above n 14, 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[26]. So are the implications of the Internet for the integrity of financial markets, for tax avoidance and tax havens[27]. Equally controversial is the impact of the Internet upon cultural sovereignty and diversity[28] 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[29], the Supreme

---

26 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).

27 Wacks, above n 14 at p 111. cf *California Software Inc v Reliability Research Inc* 631 1=Supp 1356, 1363 (C.D. Calif 1986); C Elliott, "The Internet - A New World Without Frontiers" [1998] NZLR 405 at 410.

28 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.

29 *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.

Court of that country itself recognised, that the practical consequence of its decision would reach far beyond the borders of the United States of America[30]:

> "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".

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[31]. 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 respected persons" and "inappropriate information" concerning the King of

---

30 *Reno, ibid,* at p 372.

31 China, Singapore and Germany have introduced laws. See Wacks, above n 14, at p 99.

Thailand, the Thai Royal Family and also "Heads of State of friendly foreign countries"[32]. 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 the undesirability) of censoring the international flow of data of this kind.

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 capacity of national law-makers to respond to the challenge of the Internet is nothing but

---

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

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 undoubted dangers.

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 country needs to review its laws and policies to adapt them to the new technology. In Australia, in the space of a year or two, three discussion papers have been produced by official bodies. It is highly desirable that in every country 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[33] 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 Campaign[34], as well as citizen initiatives to advocate endangered values such as privacy[35], 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

---

33 G 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>.

34 *Ibid*, at p 119.

35 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.

the OECD twenty years ago. There are serious gaps in those principles which now need attention[36].

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 ... the individual should retain the ability to disengage the feature if he or she so chooses"[37].

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. Whilst society needs to be shielded from clearly antisocial conduct, there are strong arguments for permitting, and protecting, the anonymity of most website visits[38] and providing "dungeons" and "chat

---

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

37 H H Perritt and C J Lhulier, above n 20. See also G Greenleaf, above n 11, 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.

38 G Greenleaf, above n 11.

rooms" in the web where people can communicate without fear that their interests, attitudes, beliefs and concerns will be monitored either by public or the private sector snoops[39].

6. One feature of Internet reporting is the intensification of the competition for getting the "news" first. This puts great pressure upon journalistic ethics. No public figure is entitled to protection in relation to aspects 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

---

39 *Ibid*, at p 98.

and apply just rules for its operation[40]. If it cannot, that fact itself 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[41].

---

40 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.

41 G Greenleaf, "An Endnote on Regulating Cyberspace: Architecture vs Law" (1998) 21 *Uni NSW Law Journal,* 593.