BILETA
BRITISH & IRISH
LEGAL
EDUCATION
TECHNOLOGY
ASSOCIATION

13th Annual BILETA Conference: '*The Changing Jurisdiction*'

Friday, March 27th & Saturday, March 28th, 1998.
Trinity College, Dublin.

The Death of Online Privacy?

Raymond Wacks
Professor of Law and Legal Theory
University of Hong Kong

The perils of life in cyberspace increase daily. The vulnerability of users to the monitoring of their Internet activities and the interception of their e-mail, are widely acknowledged to constitute serious violations of privacy. [1] It is these two issues that are the principal concern of this paper.

The Internet

The 'information superhighway' will eventually comprise a fibre optic network that carries - in digital bits - an almost infinite number of television channels, home shopping and banking, interactive entertainment and video games, computer data bases, and commercial transactions. This 'broadband communications network' will link households, businesses, and schools to available information resources. It is a huge and expanding empire, and I shall concentrate on only one of its colonies: the Internet. The Net interconnects innumerable groups of linked computer networks. It is a global Web of networks. Each computer in any network can communicate with computers on any other network in the system: a decentralized, unrestricted global medium of communications or what the science fiction writer, William Gibson, called 'cyberspace' that links individuals, institutions, corporations, and governments around the world. It permits the tens of millions of people with access to the Internet to exchange ideas, software, images, literature, sound, or simple e-mail. These communications are almost instantaneous, and can be directed either to specific individuals, to a group of individuals interested in a particular subject, or to the world as a whole.

The Internet began in 1969 as an experimental project of the US Advanced Research Project Agency ('ARPA'). First called ARPANET, the network linked computers and computer networks owned by the military, defence contractors, and university laboratories conducting defence related research. The network later allowed researchers across the US to obtain direct access and to use powerful supercomputers located at a few key universities and laboratories. As it evolved to embrace universities, corporations, and individuals around the world, the ARPANET came to be called the 'DARPA Internet', and finally just the 'Internet', or simply 'the Net'. It would seem that no entity - academic, corporate, governmental, or non profit -making - controls, or indeed runs, the Internet. It functions solely as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use a common data transfer protocol to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would be impossible for any single entity to regulate the information conveyed on it.

The Net has grown exponentially in the past few years. In 1981, fewer than 300 computers were linked to the Internet, and by 1989, the number stood at fewer than 90,000 computers. By 1993, however, over 1,000,000 computers were linked. It has been estimated that over 9,400,000 host computers worldwide are linked to the Internet, and this count does not include the tens of millions of personal computers used by individuals to access the Internet using modems. Reasonable estimates are that over 40 million individuals around the world can and do access the Internet. That figure is expected to grow to 200 million Internet users by the year 1999.

Two chief methods exist by which to establish a link to the Internet. First, an individual may use a computer or computer terminal that is directly, and usually permanently, connected to a computer network that is itself directly or indirectly connected to the Internet. Second, an individual can use a personal computer with a modem to connect over a telephone line to a larger computer or computer network that is itself directly or indirectly connected to the Internet. Both direct and modem connections are made available to individuals by a wide variety of academic, governmental, or commercial entities. Users often do not have their own 'username' or identification code that would indicate to others on the Internet the identity of the user.

Many users access the Internet anonymously or through a method that would not allow for clear identification by a remote content provider. With the exception of point to point mail, no information flows through cyberspace to a particular individual unless the individual requests the information. Listservs, newsgroups, chat lines, telnet, ftp, gopher and the World Wide Web all require an affirmative request by the Internet user prior to the user receiving information over the Internet. Thus, unlike radio or television, there is a significantly reduced risk that a user will receive unsolicited and undesired content.

Because information is located on millions of computers around the world, a user cannot possibly know which computers might have useful information until starting a search. Instead, the user could access any of scores of different search databases, obtain a list of sites that might be of interest, and then immediately link to one or more of the sites. Indeed, the very theory of 'hyperlinks' and the hypertext markup language (html), the foundation of the WorldWide Web, is that the user can jump from site to site to site without ever needing to know where physically in the world the next site is located. Thus, there is no way for a user to pre register with every computer that might contain useful content on a particular topic.

Privacy

Once personal information assumes the form of bits, its vulnerability to misuse, particularly on the Internet is self-evident. It is important to recognise that in the digital world the distinction between computer and telephone communication has all but disappeared. The switching systems of modern digitalised telephone systems are controlled by computers, and interception is effected by manipulation of the software on which those computers depend. Each telephone number is represented by a long code, the LEN (Line Equipment Number), which assigns functions and services to the telephone. Switching manipulation of the codes may re-route calls, re-assign numbers or effect other alterations. This facilitates an eavesdropper listening to the switch-routed call. Because computers can talk to each other through the use of modems, manipulation of switching software may be effected on the computer in question or through another computer anywhere in the world. It might be for law enforcement purposes, or it might be hacking merely as a diversion. Or there may be an economic motive. For example, a credit card thief may re-route verification calls from the credit card company to a number to which the thief has access. A telephone network is, to all intents and purposes, a giant computer linking terminals or telephones. But some technological developments have increased the difficulty of isolating individual communications. Thus unlike copper wire, fibre optics can carry thousands of conversations in a single strand of fibre.

Cookies and clickstreams

Cookies are text files written to a user's hard disk without his knowledge. They track our clickstreams and read data stored on our computer: user ID, password, preferences, lists of sites visited and perhaps more. When the user re-visits a site, his browser uploads the cookies. The ostensible purpose of cookies is to facilitate customised services to the user. A user gains the ability to select configuration options, automatic logins to subscription sites, and greater interactivity on the Web such as online shopping. It may be that the content of these unsolicited files do not include personal names or e-mail addresses, but the potential for misuse of such data is considerable.

Certain browsers do provide the means to disable cookies, but this is (deliberately?) a complex and time-consuming process, and it is bought at the cost of slower downloading without the interactive features afforded by cookies themselves. [2]

MUDs and MOOs

Apart from the problem of when it is reasonable to expect that one's conversations are 'private', the nature of communication on the Internet generates different issues and expectations, and, hence, the need for different solutions. While the monitoring of digital telephone systems (voice and fax) may appear to be similar to the sending and receiving of e-mail, the use of the Internet stretches the limits of the conventional analysis. For example, while it is simple to monitor my telephone calls or intercept my letters, the culture of the Internet invites a range of activities whose observation presents irresistible opportunities for those who wish to supervise or control the private and the sensitive.

The growing use of MUDs (multi-user domains or dungeons), MOOs (MUDs Object Oriented) and chat rooms, in which participants reveal the most intimate features of themselves (or virtual selves) is the most obvious instance of high-risk transfer of personal information vulnerable to interception or misuse. But there are others. The advent of digital cash and the various proposals to monitor or control access to certain Web sites for, say, the management of electronic copyright (ECMS), [3]require, on a practical level, a careful analysis of the requirement of anonymity and, philosophically, a consideration of the very concept of identity.

In the US, Laurence Tribe has proposed a twenty seventh Amendment to the Constitution which would provide:

This Constitution's protections for the freedoms of speech, press, petition, and assembly, and its protections against unreasonable searches and seizures and the deprivation of life, liberty, or property without due process of law, shall be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted, or controlled. [4]

This may drive the Constitution into the electronic age, but it probably fails to defend the security of data against the private hacker or the monitoring of access to data by private bodies, and conceivably even the state (though this would of course be a matter of interpretation). [5]

Anonymity and identity

Anonymity is an important value. Even in a pre-electronic age, it facilitates participation in the political process which an individual may otherwise wish to spurn. Indeed, the US Supreme Court in *MacIntyre* [6] in 1995 reaffirmed the interpretation (first articulated in *Talley v California* [7]) that the First Amendment protects the right to anonymous speech. 'Privacy' considerations are obviously germane. There are a numerous reasons why I may wish to conceal my identity behind a pseudonym or achieve anonymity in some other way. On the Internet I may want to be openly anonymous but conduct a conversation with others (with either known or anonymous identities) using an 'anonymous return address'. I may even wish no-one to know the identity of the recipient of my e-mail. And I may not want anyone to know to which newsgroups I belong or which Web sites I have visited.

There are obvious personal and political benefits of anonymity for whistleblowers, victims of abuse, those requiring help of various kinds. Equally, (as always?) such liberties may also shield criminal activities, though the right to anonymous speech would not extend to unlawful speech.

Anonymity enjoys a unique relationship with both 'privacy' and free speech. The opportunities for anonymity afforded by the Internet are substantial; I suspect that we are only on the brink of discovering its potential in both spheres. Already, the use of telephone forwarding provides a dramatic instance of how the combination of powerful encryption and digital networks communication portends dramatic changes in the way we communicate.

There is a plethora of reasons to explain the attractions of the long shadows cast by the Internet. Banking, financial, and foreign exchange transactions, tax and political risk avoidance, and jurisdiction-shopping, are already becoming commonplace features of commercial life on the Internet. 'Locational ambiguity' [8] provides a shield against both government and private intruders, but it also facilitates considerably greater access to those who need or want their services by small business, NGO's and other groups whose actual, physical addresses might otherwise inhibit or discourage such contact.

The advances, particularly, in foreign banking have spilled over into a huge international trade in securities, currency, and a host of derivatives. An Internet market in patents is planned. With strong encryption the advantages of offshore bank accounts and tax planning will no longer be the preserve of the affluent. As we

seek more congenial destinations for our assets, savings or investments, many will become financial gypsies or virtual expatriates. Place, race and gender are dissolved in cyberspace: I am no longer a white male in Hong Kong, but a shifting bit in the Internet's huge kaleidoscope. My identity ceases to be a function of my physical being.

Yet, despite these developments, conventional accounts neglect the value and importance of anonymity as a feature of the 'new privacy'. Indeed, it raises (slightly unsettling) questions about the very question of who we are, the very nature of our identity. The instability of the subject is a central theme of postmodernism. The Internet appears as a living testament to the ideas of the absence of a universal, unitary truth, and the contingency and diversity of the self that emerges from the writings of postmodernist icons such as Jacques Lacan.

Certainly, the existence of online personae conducting conversations or even relationships with others with similarly shifting identities presents a host of recondite questions which I shall not pursue here - even if I knew how. [9]

The fluidity of identity on the Internet is among its chief attractions, but there may be increasing pressure to establish who is the sender, especially for commercial and, perhaps, law enforcement, purposes. Digital authentication is likely to grow in importance as more business is conducted online, a matter I return to below.

Encryption

Though there is plainly a role for the law, the most effective means of enhancing both 'privacy' and free speech on the Internet is the use of encryption. The use of strong encryption to protect the security of communications has been met by resistance (notably in the US and France) and proposals either to prohibit encryption altogether, or, through means such as the Clipper Chip or public key escrow, to preserve the power to intercept messages.

The US has enacted legislation to ensure that telecommunications systems are designed to facilitate government interception. The US Digital Telephony and Communications Privacy Improvement Act 1994 does not wholly undermine the integrity of communications on the Internet: it excludes on-line information services, electronic messaging services, and electronic publishing. But it does provide for a subpoena process for obtaining customer information on these on-line services.

The battle has been joined between law enforcers and cryptographers; it is likely to be protracted, especially since enthusiastic would be too mild a word to describe the manner in which the culture of strong encryption has been embraced by ordinary computer users, especially in the US: Phil Zimmerman's encryption software, PGP ('Pretty Good Privacy') may be generated in less than 5 minutes, and is freely available on the Internet.

A central feature of modern cryptography is that of the 'public key'. A lock-and-key approach is adopted to telecommunications security. The lock is a public key which a user may transmit to recipients. To unlock the message, the recipient uses a personal encryption code or 'private key'. Public key encryption significantly increases the availability of encryption/identification, for the dual key system allows the encryption key to be made available to potential communicants while keeping the decryption key secret. It permits, for instance, a bank to make its public key available to several customers, without their being able to read each others' encrypted messages.

The Clipper Chip

On 16 April 1993 President Clinton announced 'a new initiative that will bring the Federal government together with industry in a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement'. The Clipper Chip is the US government designed encryption system for encoding and decoding telephone calls and e mail to protect the communication from interception. It permits the government to retain a 'back door key' in order to intercept messages from 'gangsters, terrorists, and drug dealers'. The initiative encountered fierce opposition, despite the view of the National Security Agency which argues that non escrowed encryption technology threatens law enforcement and national security.

Clipper is a hardware microcircuit based upon the classified 'Skipjack' encryption algorithm developed by the US National Institute of Standards and Technology to scramble telecommunications. The Clipper Chip would create a government encryption standard to facilitate the government descrambling voice communications encrypted with the chip, thus constituting an electronic 'trapdoor' enabling the government to eavesdrop on digital communications. The chip could be used in relatively inexpensive encryption devices that can be attached to an ordinary telephone. The Clipper Chip applies encryption to voice messages, 'Capstone' is the related scheme for the encryption of data.

The US government claimed that the proposal provides merely a new means by which to intercept communications, not an extension of legal authority to do so. It also acknowledged that to win public trust, the government would not abuse the proposed capability to decrypt private transmissions without judicial warrant, as the law now requires. The means by which such trust would be gained is the 'key escrowing': two 'trusted third parties' are designated, each of whom holds a piece of the decryption key. The communication in question can be decrypted only by obtaining both pieces of the decryption key, under legal authority.

Much of the opposition to the Clipper Chip rests on the concern that the Clipper encryption standard would become mandatory, and whether other encryption might be prohibited. The principal commercial objection is that foreign users of telecommunications equipment will not purchase United States equipment loaded with Clipper Chips because it would provide United States government agencies with a back door to their electronic communications. The US administration has now agreed instead to accept seven key principles as the framework to develop an encryption system. It should be (1) voluntary; (2) exportable; (3) not reliant on a classified algorithm; (4) implementable in software, firmware, hardware or any combination; (5) permit the use of private-sector key escrow agents; (6) contain safeguards to provide key disclosure only by court orders with audit procedures; and (7) hold escrow holders liable for unauthorised key release. [10]

Trusted Third Parties

Echoes of this controversy are now beginning to rumble in Britain. The Government has recently proposed a system of 'trusted third parties' (TTP) who would furnish transmission services for encrypted messages, provided that secret keys be disclosed under a warrant procedure. Ostensibly, this regulatory framework suggested by the Department of Trade and Industry is designed largely to control crime on the Internet which, it claims, undermines the development of electronic commerce (see below). The use of TTPs would be voluntary, TTPs would be licensed, and other safeguards are proposed. Criminal sanctions would be imposed on TTPs improperly disclosing a client's key; they would be strictly liable for keeping clients' keys secure. The Government claims it has no intention of accessing private keys merely for integrity functions. And both the Data Protection Act and Computer Misuse Act would apply to TTPs. [11]

Despite these safeguards, there remains the obvious risk that the determination of who or what is to be the central repository is made by the administration. Moreover, since the system is a volunatry one, lawbreakers would steer well clear of it and employ other strong encryption such as PGP. The scheme devotes 'no space to the importance of privacy and anonymity on the Internet. Anonymous speech is very important, but because it is not a commercial issue, it has been excluded from the content of the consultation paper (see paragraph 16, and 36). This is a sad reflection on the previous UK government's sense of priorities.' [12]

Electronic commerce

Technological solutions are especially useful in concealing the identity of the individual. Weak forms of digital identities are already widely used in the form of bank account and social security numbers. They provide only limited protection, for it is a simple matter to match them with the person they represent. The advent of smart cards that generate changing pseudo-identities will facilitate genuine transactional anonymity. 'Blinding' or 'blind signatures' and 'digital signatures' will significantly enhance the protection of privacy. A digital signature is a unique 'key' which provides, if anything, stronger authentication than my written signature. [13] A public key system involves two keys, one public, the other private. The advantage of a public key system is that if you are able to decrypt the message, you know that it could only have been created by the sender.

There is little doubt that in time electronic cash (e-cash) will become the standard way of transacting business in cyberspace. David Chaum's Digicash employs a blinding technique that sends randomly encrypted data to my bank which then validates them (through the use of some sort of digital money) and returns the data to my hard disk. Only a serial number is provided: the recipient does not know (and does not need to know) the

source of the payment. This process affords an even more powerful safeguard of anonymity. It has considerable potential I think in electronic copyright management systems (ECMS) with projects such as CITED (Copyright in Transmitted Electronic Documents) and COPICAT, being developed by the European Commission ESPIRIT programme. Full texts of copyrighted works are being downloaded and marketed without the owner's consent or royalty being paid. These projects seek technological solutions by which users could be charged for their use of such material. This 'tracking' of users poses an obvious danger: my reading, listening, or viewing habits may be stored and access to them obtained for potentially sinister or harmful purposes. Blind signatures seem to be a relatively simple means by which to anonymise users.

The paramount question is: is my identity genuinely required for the act or transaction concerned? It is here I think that the widely accepted core of data protection principles may be of assistance.

Data Protection

At the core of all data protection legislation, since the OECD guidelines of 1980, is the proposition that data relating to an identifiable individual should not be collected in the absence of a genuine purpose and the consent of the individual concerned. At a slightly higher level of abstraction, it encapsulates the principle of what the German Constitutional Court has called 'informational self-determination' [14] - a postulate that expresses a fundamental democratic ideal. Adherence to, or more precisely, enforcement of, this idea (and the associated rights of access, correction) has been mixed in the nearly 30 jurisdictions (most recently joined by my own) [15] that have enacted data protection legislation.

Most of these statutes draw on the OECD guidelines of 1981 and those formulated by the Council of Europe in 1980. The European Union 1995 Directive on Data Protection provides a comprehensive framework binding on member states. They have three years to implement its provisions.

The enactment of data protection legislation is driven only partly by altruism. The new information technology disintegrates national borders; international traffic in personal data is a routine feature of commercial life. The protection afforded to personal data in Country A is, in a digital world, rendered nugatory when it is retrieved on a computer in Country B in which there are no controls over its use. Hence, states with data protection laws frequently proscribe the transfer of data to countries that lack them. Indeed, the European Directive explicitly seeks to annihilate these 'data havens'. Without such legislation, countries risk being shut out of the rapidly expanding information business.

Thus, section 25 of the European Directive specifies that any transfer of personal data which is being processed or is to be processed after its transfer must attract an adequate level of protection by the jurisdiction to which it is sent. The adequacy of protection is to be evaluated by reference to the nature of the data, the purpose and duration of the proposed processing, the country of origin and of final destination, the general or sectoral regulation in the jurisdiction in question, and the nature and scope of security measures.

It is hard to overstate the importance, in particular, of the use limitation [16] and purpose specification [17] principles as canons of fair information practice. Together with the principle that personal data shall be collected by means that are 'lawful and fair in the circumstances of the case' [18] - as expressed in Hong Kong's Personal Data (Privacy) Ordinance, it provides a framework for safeguarding the use and disclosure of such data, but also (in the fair collection principle) for limiting intrusive activities such as the interception of e-mail messages. [19]

Personal data may be used or disclosed only for the purposes for which the data were collected or for some directly related purposes, unless the data subject consents. 'Personal data' means any data '(a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.'

While the administrative regime established under the ordinance has certain limitations, [20] it goes a long way towards regulating the misuse of personal data on the Internet. They require rejuvenation where they already exist, and urgent adoption where they do so only partially (most conspicuously in the United States). [21] Moreover, as suggested above, they may be able to provide complementary safeguards for individual privacy in cyberspace.

The Net contains a vast amount of personal data (that is, information about identifiable individuals in

accessible form). Since a Web server collects and stores such data, it is presumably controlled by the UK Data Protection Act. [22] If so, the server would need to register as a 'data user', and several of the provisions of that law would apply to its operation. My university, for example, displays information about me (my educational qualifications and history, publications, etc) on its Web site. The legislation (including the data protection principles, right of access and correction, and so on) should protect me against transfer of the data out of the jurisdiction). [23]

At the heart of Hong Kong's Personal Data (Privacy) Ordinance is the principle that personal data shall be collected by means that are 'lawful and fair in the circumstances of the case.' [24] In respect of the use and disclosure of such data, they may be used or disclosed for the purposes for which the data were collected or for some directly related purposes, unless the data subject consents. 'Personal data' means any data '(a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.'

While the administrative regime established under the ordinance was not fashioned to afford relief or restrain threatened misconduct of this kind, [25] in the absence of more explicit remedies, it could easily be amended to assist victims of both unfair intrusion and disclosure.

Conclusion: A Reasonable Expectation of Privacy Online?

The telephone, the radio, and the camera provide snoopers with helpful means of invading our privacy, yet it is unthinkable that we could dispense with them. We have learned to adjust our expectations when we use them. And if we wish to protect our personal information, we must recognise the need for vigilance. The Internet offers hitherto unimagined prospects for communication, education, commerce, and entertainment. But it also poses significantly greater threats to our privacy. At the very least, Netizens need to adopt the following Ten Commandments to safeguard whatever vestiges of privacy still remain: [26]

1. Assume that your online communications are not private unless you use powerful encryption. Do not send sensitive personal information (phone number, password, address, credit card number, vacation dates) by chat lines, forum postings, e mail or in your online biography.
2. Be cautious of start up software that makes an initial connection to the service for you. Often these programs require you to provide credit card numbers, checking account numbers, NHS numbers, or other personal information, and then upload this information automatically to the service. Also, these programs may be able to access records in your computer without your knowledge.
3. Public postings made on the Internet are often archived and saved for posterity. For example, it is possible to search and discover the postings an individual has made to Usenet newsgroups. This information can be used to create profiles of individuals for a variety of purposes, such as employment background checks and direct marketing.
4. Be aware that online activities leave electronic footprints for others to see, both at your own service provider and at any remote sites you visit. Your own service provider can determine what commands you have executed and track which sites you visit. Web site operators can often track the activities you engage in on their site, particularly at sites which ask you to 'register' or otherwise provide personal information. Some Web browsing software transmits less information to remote sites than other software. You can avoid leaving tracks when you send e mail messages by using anonymous remailers.
5. The 'delete' command does not make your messages disappear. They can still be retrieved from back up systems.
6. Others' online identities are not always what they seem. Many network users adopt one or more online disguises.
7. Be aware of the possible social dangers of being online: harassment, stalking, being 'flamed' (emotional verbal attacks), or 'spamming' (being sent frequent unsolicited messages). Women can be particularly vulnerable if their e mail addresses are recognizable as women's names. Consider using gender neutral online IDs.
8. Take advantage of privacy protection tools. There are several technologies which help online users protect their privacy: Encryption, anonymous remailers, and memory protection software.
9. Memory protection software helps to prevent unauthorised access to files on the home computer. For example, one program encrypts every directory with a different password so that to access any

directory you must log in first. Then, if an online service provider tries to read any private files, it would be denied access. These programs may include an audit trail that records all activity on the computer's drives.

10. If you publish information on a personal Web page, note that direct marketers and others may collect your address, phone number, and any other information that you provide.

In *Malone*, Megarry VC sounded a slightly dystopian note:

> It seems to me that a person who utters confidential information must accept the risk of any unknown overhearing that is inherent in the circumstances of communication. [27]

He was, of course, referring to telephone communication, but it would appear that twenty years later, one is driven to the same unfortunate conclusion in respect of the Internet. Thus, for example, E-mail messages are little more than the digital version of the postcard. It should be assumed - unless the message is encrypted - that they will be read by persons other than the intended recipient.

Neither at work nor at home, [28] are we entitled to assume that our online applications are safe. Under these circumstances, we have little choice but to look to both technology and the law to provide shelter. Ironically, technology generates both the malady and part of the cure. And the law is rarely an effective tool against the dedicated intruder. Yet the advances in protective software along with the fair information practices adopted by the new European Directive on Data Protection, and the laws of several jurisdictions, [29] afford a normative framework for the collection, use and transfer of personal data. We shall nevertheless need to re-think the way in which we communicate and, especially, the legal and moral obligations generated by our networked society.

- Return to index

Notes

(1). I draw here on R Wacks, 'Privacy in Cyberspace: Personal Information, Free Speech, and the Internet' in P Birks (ed), Privacy and Loyalty (Oxford: Clarendon Press, 1997).

(2). Adriana is a cookieless browser that enables users to disable the cache in their hard disks, which tracks visited Web pages. Through programs such as NSClean and IEClean, (products of Netscape and Internet Explorer respectively) it is also possible properly to erase the site history on the hard disk, though it potentially lives on with the ISP. A Web site called Anonymizer (http://www.anonymizer.com) is described by its inventor, Justin Boyan, as an Internet 'caller ID block'. Rather than a user retrieving Web pages, he instructs Anonymizer to do so. It relays the page back to the browser, thereby acting as a proxy to block unwanted cookies. Doubtless there is already software available to kill the proxy!

(3). The IMPRAMATUR Project (Intellectual Multimedia Property Rights Model and Terminology for Universal reference) is a good example for such an initiative. Launched in 1989 under the aegis of the ESPRIT programme, it is co-ordinated by the UK Authors' Licensing and Collecting Society which represents the interests of a variety of IT and telecommunications industries in Europe, the United States, and Japan. It attempts to devise means by which to reconcile the needs of users and the rights of intellectual property owners. For a general account of the kinds of copyright problems in cyberspace, see Jane C Ginsburg 'Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace' (1995) 95 Colum LR 1466.

(4). Laurence H Tribe 'The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier' Keynote Address at the First Conference on Computers, Freedom and Privacy, 26 March 1991. It may be found (along with much else) at the CFP Web site, the most recent of which is http://swissnet.ai.mit.edu/switz/cfp96/. Other useful addresses on http://www are epic.org/privacy [(a clearing house for information on the major privacy organisations run by the Electronic Privacy Information Center (EPIC)]; vortex.com/privacy. 2020tech.com/maildrop/privacy, and privacy.org.pi. (Privacy International)].

(5). Similarly, attempts have been made to extend First Amendment theory to questions of controlling the content of information (especially pornographic or subversive) on the Internet. Recently the authorities in China, Singapore, and Germany have demonstrated, in different ways, their intention to censor what passes in or out of their territories via the Internet. And the current challenge to the constitutionality of the American Communications Decency Act (which is designed to protect users from pornography on the Internet) illustrates that this issue is unlikely to disappear in the foreseeable future. In the case of the United States (which, as in most things, will be the first to have to grapple with this question), we should expect a lively contest between the 'right of privacy' and free speech on the Internet.

(6). *McIntyre v Ohio Elections Commission* (1995) 115 S Ct 1151. The Court held that anonymous speech about important public issues was 'core political speech' and that any attempt by a state to regulate this speech must be 'narrowly tailored' to achieve the state's legitimate interest in prohibiting unknown authors from providing the electorate with fraudulent and libellous information. The Court found that the prohibition contained in the Ohio statute was not narrowly tailored because it punished all unknown authors, not only those who attempted to publish false and misleading information.

(7). 362 US 60 (1960).

(8). Ibid.

(9). A good stab at it has been made by Sherry Turkle, especially in her Life on the Screen: Identity in the Age of the Internet (New York: Simon & Schuster, 1995) in which she applies Lacanian ideas to the Internet. See too T Druckery (ed), Electronic Culture: Technology and Visual Representation (Ontario: Aperture, 1996), L H Leeson (ed), Clicking In: Hot Links to a Digital Culture (Seattle: Bay Press, 1996).

(10). In October 1997 the European Commission issued a paper, 'Towards A European Framework for Digital Signatures And Encryption' which expresses the view that key escrow and key recovery systems are inefficient and ineffective.

(11). *Licensing of Trusted Third Parties for the Provision of Encryption Services*, Public Consultation Paper on Detailed Proposals for Legislation, March 1997, Information Security Policy Group, Department of Trade and Industry.

(12). Y Akendiz, 'No Chance for Key Recovery: Encryption and International Principles of Human and Political Rights', [1998] 1 Web JCLI.

(13). The DTI consultation paper (note 11 above) floats the idea of a rebuttable legislative presumption that a document has been signed by a person named in a certificate issued by a licensed TTP who provided encryption services for that document, paras 51-53, and Annex A, p 21.

(14). *Volkszahlungsurteil* (National Census Case) (1983) 65 BVerfGE 1, 68-9, cited in S Simitis 'Reviewing Privacy in an Information Society' (1987) 135 University of Pennsylvania Law Review 707, 734.

(15). The Personal Data (Privacy) Ordinance of 1995, most of whose provisions are expected to come into force by the end of 1996, is almost certainly the most far-reaching of existing data protection statutes. Hong Kong should encounter no difficulty in complying with the stringent terms of the European Directive on Data Protection of 1995. For a brief overview of the legislation and some of the factors leading to its enactment, see R Wacks, 'Data Privacy: Reforming the Law' (1996) 26 Hong Kong Law Journal 149.

(16). The principle is expressed in the following form by the OECD Guidelines: 'Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with (the purpose specification principle) except: (a) with the consent of the data subject; or (b) by the authority of law.'

(17). This is expressed as follows in the OECD Guidelines: 'The purposes for which data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.'

(18). Section 2(1). See R Wacks, 'Data Privacy: Reforming the Law' (1996) 26 HKLJ 149.

(19). Interception, like hacking, calls for its own elaborate legal control. For a detailed discussion of the issues, see Report on Privacy: Regulating the Interception of Communications, The Law Reform Commission of Hong Kong, December 1996. The forms in which pre-Net invasions of privacy may take are best clustered around the wrongful acts of 'intrusion' and 'disclosure'. See generally R Wacks, The Protection of Privacy (London: Sweet & Maxwell, 1980); R Wacks, 'The Poverty of "privacy"' (1980) 96 LQR 73; R Wacks, Personal Information: Privacy and the Law (Oxford: Clarendon Press, 1993); R Wacks (ed), Privacy (2 vols), International Library of Essays on Law and Legal Theory (London: Dartmouth, 1993; New York: New York University Press, 1993).

(20). Among the important limitations of the ordinance is that it is confined to data in a recorded form. There is no protection of the data subject unless the data user converts the data into a form in which access to or processing of them is practicable, s 2(1). Moreover, the data protection principles are just that; they are not rules. The burden is also placed on the data subject to show that the data are indeed 'personal data', as defined. He must therefore demonstrate, to the satisfaction of the Privacy Commissioner, that the data are not covered by one of the exemptions in the ordinance. None of these shortcomings is incapable of simple amendment if specific legislation is not passed. Indeed, there is a good deal to be said for addressing the central problems of privacy protection (or what I prefer to call the protection of 'personal information') under the rubric of fair information practices, including the growing challenges of privacy of e-mail and on the Internet. See R Wacks, 'Privacy in Cyberspace: Personal Information, Free Speech, and the Internet' (note 1 above). See generally M Berthold and R Wacks, *Data Privacy Law in Hong Kong* (Hong Kong: FT Law & Tax Asia Pacific, 1997).

(21). There are several signs that even in the recalcitrant United States a belated recognition is emerging that a comprehensive legal regime is required to provide individuals with the right to control the collection and use of their personal Data. See, for example, Susan E Gindin, 'Lost and Found in Cyberspace: Informational Privacy Rights in the Age of the Internet' (1997) <http://www.info-law.com/articles.html>.

(22). This is the view of the Data Protection Registrar in her 11th Annual Report, June, 1995, pp 76-77.

(23). The UK Act does not define 'transfer', but it has been suggested that the process by which data are passed on demand from a Web server to a Web browser, constitutes more than mere 'disclosure'. If this is indeed a 'transfer' it follows that if personal data are 'held on an open access Web server, there would be no way for the owner of that Web server to avoid the transfer of that personal data to any individual with full Internet access in any number of countries outside the UK.' It would also seem to be the case that such Web pages could only comply with the law if it were possible for Web servers to have entries in the data users register of "all other Web users" and "the world" respectively. Such a solution would seem to be so wide-ranging as to render this part of the DPA 1984 meaningless,' Andrew Charlesworth 'When the Personal Becomes Public' (1996) THES 12 July. In *R v Brown* [1996] 2 WLR 203 the House of Lords (by 3-2) held that 'use' in s 5(2)(b) of the DPA 1984 was to be given its natural and ordinary meaning so that merely retrieving data on a screen did not constitute 'use' of that data; it had to be shown that the defendant actually made use of them. This seems (despite Lord Hoffmann's unimpeachable logic) to produce a distinction so fine as to frustrate an important objective of the legislation. The Hong Kong Personal Data (Privacy) Ordinance of 1995 defines 'use' to include both transfer and disclosure of personal data. See M Berthold and R Wacks *Data Protection: A Practical Guide to the Hong Kong Law* (Hong Kong: Pearson International, 1997).

(24). Section 2(1). See R Wacks, 'Data Privacy: Reforming the Law' (note 15 above).

(25). Among the important limitations of the ordinance is that it is confined to data in a recorded form. There is no protection of the data subject unless the data user converts the data into a form in which access to or processing of them is practicable, s 2(1). Moreover, the data protection principles are just that; they are not rules. The burden is also placed on the data subject to show that the data are indeed 'personal data', as defined. He must therefore demonstrate, to the satisfaction of the Privacy Commissioner, that the data are not covered by one of the exemptions in the ordinance. None of these shortcomings is incapable of simple amendment if specific legislation is not passed. Indeed, there is a good deal to be said for addressing the central problems of privacy protection (or what I prefer to call the protection of 'personal information') under the rubric of fair information practices.

(26). Adapted from 'Privacy in Cyberspace: Rules of the Road for the Information Superhighway', Fact Sheet No 18, Privacy Rights Clearinghouse, <http://www.privacyrights.org/fs/fs18-cyb.html>

(27). *Malone v Commissioner of Police of the Metropolis (No 2)* [1979] 2 All ER 620 at 646. Cf Malone v

United Kingdom (1984) 7 EHRR 14.

(28). See M S Dichter and M S Burkhardt, 'Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age' (paper delivered at the Fourth Annual Conference of the American Employment Law Council, October 1996) at <http://www.mlb.com/speech1.htm>; D R McCartney, 'Electronic Surveillance and the Resulting Loss of Privacy in the Workplace' (1994) 62 Univ Missouri-Kansas Law Review 858; International Labour Organisation, 'Monitoring and Surveillance in the Workplace' (1993) 12 Conditions of Work Digest. Employers increasingly claim a right to monitor the private e-mail and other activities conducted by means of the employer's equipment. Lawsuits by employees have so far been conspicuously unsuccessful. It is clear that a code of practice needs to be agreed between workers and employers specifying - in advance - precisely what communications are susceptible to interception. For a specimen see Dichter and Burkhardt, op cit, pp 25-19.

(29). The UK's Data Protection Bill 1998, is available at <http://www.parliament.the stationery office.co.uk/pa/ld199798/ldbills/061/1998061.htm>and <http://www.parliament.the stationery office.co.uk/pa/ld199798/ldbills/061/1998061.htm>

- Return to index
