1

A charter for citizens of the global information society

Julie Cameron and Karin Geiselhart***
** Info.T.EC Solutions Pty Ltd*
P.O. Box K21 Haymarket, Sydney, NSW 2000, Australia
Phone: +61 2-93269430; Fax +61 2-2181508
Email: cameronj@acslink.aone.net.au
*** Student, University of Canberra,*
Canberra, ACT 2600, Australia
Email: k.geiselhart@student.canberra.edu.au

Abstract

New ethical issues related to the global information society have emerged. Extraterritoriality and legal ambiguity are consequences of the global information society and cyberspace. This discussion paper summarizes key ethical issues that need to be addressed in a charter for citizens of the global information society. For each issue, the main implications for citizens of nations and of cyberspace are discussed and statements of principle are developed. These principles, set out as a charter for citizens, are intended for use as: guidelines by law-makers and decision-makers in government and industry; an ethical framework for possible future international legislation; and as benchmarks for citizens and cybercitizens in assessing their rights and obligations in relation to the global information society and cyberspace.

INTRODUCTION

The power of integrated information and communication technologies to collect, store, combine, manipulate and disseminate data to and from any part of the world now affects every individual, regardless of their personal involvement with cyberspace. Technologies like space-based surveillance, satellite communication,

An Ethical Global Information Society J. Berleur & D. Whitehouse (Eds.)
© 1997 IFIP. Published by Chapman & Hall

direct broadcasting and portable equipment allow information collection and flow to transcend national and geographical borders.

High speed computers combined with massive data storage capacity, an unparalleled ability to integrate complex information systems and the power to digitize and analyze data from audio, visual and other media provide the potential for total mastery over the information of all people and all nations. Just as nuclear dominance was the key to coalition leadership in the old era, information dominance will be the key in the information age (Nye and Owens, 1996, p. 27). A global information society affects the balance of power and moves control from within nations.

In this new global information society, cyberspace is defined as the electronic environment established by and/or within the information and communications technologies and infrastructure and associated peripheral equipment. It is a non-specific, fluctuating, separate space where transactions and events occur outside the jurisdiction of the laws of individual nations. Individuals, organizations and governments increasingly engage with this electronic environment and are affected by it directly or indirectly. Indirect effects of cyberspace include unjust denial of access for individuals to finance or employment due to inaccurate electronic data, and threats to physical security and well-being due to activities like net stalking. Interaction in cyberspace may involve citizens and technical infrastructure from numerous nations concurrently. Global laws do not exist. Global mechanisms for governing the cyber realm have not been established. The result is extraterritoriality and legal ambiguity.

In the Oxford Dictionary, society means a social mode of life, the customs and organization of a civilized nation or an association of persons united by a common aim or interest or principle. Therefore cyberspace has citizens - citizens that may be individuals, organizations or governments. And citizenship of a nation and of cyberspace can be concurrent. Rights and obligations relate to roles both as citizens of a particular nation and of cyberspace, with an over-riding responsibility to citizenship of the global society. But, what is cybercitizenship in the global information society? The Oxford Dictionary defines citizen as a freeman of a city or member of a state. Traditionally a citizen is acknowledged by the law of a nation as a member of that particular country and subject to its laws. When citizenship is a local, physical concept the obligations and rights associated with being in a defined geographical area are specified. But in the information society individuals, organizations (including corporations) and governments can act and interact outside geographical constraints. Rights and obligations are not clearly defined either for individuals or collectives. So far it is established only that cybercitizens must pay suppliers of access services, obey the rules of their geographic society related to the Internet and global information and observe netiquette.

Democracy refers to the right of individuals to influence by lawful means issues affecting their lives and well-being. This paper assumes that electronic information and cyberspace should empower citizens and increase opportunities to influence and participate in the government of nations and cyberspace. We need to avoid the creation of cyberslaves - those who use cyberspace but are unaware of the issues and risks (for example, losing money if their cyberbank becomes insolvent) and have no influence on decisions and events that impact on them. Cybercitizens are

powerless unless they are able to participate in the governing of the global commons.

Options for setting out the rights and obligations of citizens can be listed in order of enforceability:

- Principles which are generally statements that may provide international guidance, or act as a reference document, or provide a basis for the development of legal instruments in particular jurisdictions (for example, the Organization for Economic Co-operation and Development (OECD) Privacy Principles).
- Public policies that may incorporate aspects of acceptable behaviours, practice and standards.
- Codes of conduct incorporating ethical principles but focusing on behaviours, outputs and quality of service for the interpretation of substantive behaviours. Although they are usually used as standards for self-regulation by industries or professions, they may also be used as guidance in external regulation (for example, by courts assessing what comprises negligent behaviour).
- Guidelines that may be legal within a single jurisdiction and used to provide guidance, legal meaning and relevance, even though they are generally not enforceable.
- Legal instruments which are generally enforceable, provided they are drafted correctly and courts are sufficiently qualified to assess the matters bought before them (Cameron *et al.*, 1992).

Because of problems related to establishing a universal ethical regime in diverse cultures (Berleur and d'Udekem-Gevers, 1996) and the nature of the global information society, the establishment of principles is considered the most appropriate form for setting out the rights and responsibilities of citizens.

The principles set out in this paper are intended to form the basis of a charter for citizens of the global information society. The principles are intended for use as: guidelines by law-makers and decision-makers in government and industry; an ethical framework for possible future international legislation; and as benchmarks for citizens and cybercitizens in assessing their rights and obligations in relation to the global information society and cyberspace.

ASSUMPTIONS AND METHODOLOGY

Principles implicitly and explicitly assume values. The values espoused in these principles reflect the experience of sophisticated users of integrated information and communications technologies and cyberspace. Globalization and transborder data flow has occurred so fast that few nation states have debated and/or understood the consequences. Maritime nations developed laws of the high seas under similar circumstances.

The various declarations of the United Nations and statements like the OECD Principles are based on the premise that some values are universal. International protocols that assume particular actions do not promote international well-being (for example, actions degrading air quality). This paper assumes that all individuals in all societies have the rights set out in the Declaration of Human Rights. The charter aims to enhance the well-being of all citizens throughout the world. The objectives of the principles are to promote a social sustainable

development (Berleur and d'Udekem-Gevers, 1996, p. 11). It is acknowledged that despite the precedents for statements of conviction with international relevance, if principles are to be universal and applied internationally, ethical and cultural diversity must be recognized. Situations and circumstances vary. The preamble to the charter therefore provides for justification and exceptions.

This paper was prepared using the following methodology:

- Placement of information about the Corfu conference and an abstract of a proposed conference paper on the Australian Computer Society's World Wide Web (WWW) page with an invitation to participate in writing the paper.
- In order to identify issues and appropriate Principles, the rights and obligations set out in various ethical statements and codes were examined by the principal author. Key source material was published (Berleur, J., this volume; Berleur and Brunnstein, 1996; Australian Privacy Charter Council, 1994, located on the World Wide Web, or distributed electronically, for example, Clarke 1996, WWWa; 1996, WWWb; Durango Declarations, 1995, WWW; Merel 1996, WWW; Kling 1996).
- A general literature search of CD-Rom databases, Internet World Wide Web sites and published journals and books by the principal author. (Material on web sites deleted or moved by 30 November 1996 is excluded.)
- Preparation of a draft paper by the principal author.
- Circulation of the draft paper internationally to 49 key individuals with a known interest in and knowledge of the topic resulted in valuable comments and references.
- Placement of the Draft Paper: Democracy and Cyberspace - A Charter for Citizens by Julie Cameron on a World Wide Web site http://www.-msj.com.au/ELSIC/Corfu97.html in October 1996. The paper was directly linked to the Australian Computer Society web page, and the ELSIC site and comments were invited via email link to the author. No email feedback was received. A count of visits to the paper was not available.
- Amendment of the draft in accordance with electronic material and comments received. All key contributors have been acknowledged and the main contributor is named as co-author.

ISSUES

Justification and Exceptions

In a diverse, complex world it would be unrealistic to establish a set of principles relating to a global information society that apply to all situations and are acceptable to all nations. But in order to protect citizens, any exceptions must be justified and reflect the level of risk to society. 'Exceptions must not interfere with universally accepted human rights. Exceptions to the Principles must be clearly stated, made in accordance with law, proportional to the necessities giving rise to the exception, and compatible with the requirements of a democratic society' (Australian Privacy Charter Council, 1994, Principle 1). Not every law of every nation is a just law. Not every nation is democratic.

Preamble to the Charter: Exceptions to the Principles set out in this Charter must be justified, clearly stated, made in accordance with law, proportional to the necessities giving rise to the exception, and compatible with the requirement to enhance human rights.

Ethics and Protection from Cybercrime

Cyberspace can obviously be used for good or evil. Misuse and abuse of electronic information and cyberspace ranges from unethical behaviours to criminal activities. 'Criminal exploitation is clearly a problem, and there are other concerns too; for example, the norms of human interaction are less likely to be observed in such environments. Electronic violence is in its infancy, but viruses, rumour-mongering, hate-mail and mailbox bombardment are all describable phenomena, and may graduate from art-forms to techniques' (Clarke, 1996 WWWa).

Although it is recognized that currently an international agreement on ethics ... is unachievable (Berleur and d'Udekem-Gevers, 1996, pp. 4-5) the International Federation for Information Processing (IFIP) Ethics Task Group's analysis of 30 codes of member computer societies revealed a consensus on some shared principles (Berleur, 1996b, p. 242). Respect for privacy, accuracy, property and accessibility is required by most codes. To retain the credibility of information, integrity and quality of digital data must be protected by individuals, organizations and governments. Safeguarding the accuracy of information is a core responsibility of individual and collective cybercitizens. False and inaccurate information in the information age can be considered as equivalent to counterfeit currency.

Even though the laws of nations do not keep pace with developments in criminal activity related to the global information society and cyberspace, and the concepts of ethics and instruments designed to deal with cybercrime vary with culture and type of behaviour they are intended to encourage or prevent, cybercitizens are aware of right and wrong. There appears to be a broad consensus that actions that would be crimes outside the electronic environment should be considered as cybercrime (for example, sabotage, forgery, fraud, theft, espionage) (Berleur and Brunnstein, 1996, pp. 260-1). There are well recognized statements of agreement related to information and communications security (such as the OECD Guidelines for the Security of Information Systems). The main risks to cyberspace security relate to insertion of false data; release or insertion of harmful software programs; destruction of valuable data and programs; manipulation and/or disruption of computer and communication systems; and misuse by, for example, information brokers, private detectives, foreign embassies and organized crime. Cybercrime must be punished in the same way as all other criminal activity and be subject to the laws of nations.

In addition to ethics directly related to electronic information and cyberspace, the information technology and communication industries need to consider issues like the environment (like manufacture and disposal of equipment, use of electricity and other resources) and to promote sustainable economic and social development.

Principle 1: Individual and collective cybercitizens must protect the accuracy and integrity of digital information, adhere to all relevant ethical principles, codes and guidelines and uphold the legitimate laws of nations.

Equity of Access to Cyberspace and Electronic Information

Equity of access to cyberspace is of international concern. The information rich and information poor are familiar concepts that apply to individuals, communities, organizations and nations. Access to cyberspace is determined by access to technical infrastructure and electronic information. Even if access to cyberspace is achieved, access to electronic information is not guaranteed.

Access to technical infrastructure and technology

Access to cyberspace depends on the availability and accessibility of technical infrastructure, access to appropriate information and communication technology, and technical skill. Some countries and groups within nations (like rural communities) lack suitable technical infrastructure. Access by some individuals, communities and organizations is limited because of the costs of information technology and communications. Recognizing these facts, the United States Federal-State Board on Universal Service, set up under the Telecommunications Act of 1996, developed draft recommendations to support programs to ensure access to telecommunications for low income consumers and discounts to key community groups (Benton Foundation, 1996, WWW). Verbal accounts of experiments indicate that linking members of disadvantaged groups to the Internet appears to have positive affects on self-esteem.

Discrimination on grounds like sex, age, race, religion or physical disability limits equality of access to cyberspace technology. Equity of access to cyberspace among all citizens should be a goal of education systems. Issues like poverty and illiteracy have obvious relevance to access and realistically other basic human rights may be more significant in some countries (such as freedom from hunger).

Access to electronic information

Information available on the Internet is voluminous, frequently difficult to find, peripatetic, transitory, often fragmented and of varied quality. Equity of access to meaningful electronic information depends on the acquisition and transfer of sophisticated search skills including the ability to discriminate among sources and knowledge of electronic conventions and practices.

There is every danger that pricing information services and placing information and its associated technologies in the market place will ensure the development of an information poor group within society who are unable to capitalize on the benefits of freely available information (Burton, 1992, p. 89). The social impact of any bit tax (a tax on information sent over the Internet) needs to be carefully assessed. Any trend to charging for access to information currently available free of charge in the public domain, via the Internet or published in books that can be accessed free of charge through libraries would exacerbate the disadvantage of those unable to pay.

Governments are major collectors of information. As governments are funded by citizens, '(n)on-personal government information should be freely available unless someone in authority can show it should be restricted. Technology should be used to distribute information to citizens not simply to record information about

them' (Burton, 1992, p. 89). But the trend of governments to privatize functions and outsource activities means that information formerly held by government and available publicly is no longer accessible. It is argued that some databases held by private sector organizations should be freely accessible due to the public interest (for example, toxic emissions and chemical hot spots). But the World Intellectual Property Organization (WIPO) has prepared a treaty that proposes new property rights to database owners. If adopted, this treaty may restrict access to information currently available in the public domain (World Intellectual Property Organization, 1996, WWW).

Principle 2: Nations should aim at equity of access to electronic information and cyberspace for all their citizens without discrimination.

Freedom from Surveillance and Rights to Privacy

Principle 3 of the Australian Privacy Charter states that people have a right to privacy and the right to conduct their affairs free from surveillance or fear of surveillance. Rights to privacy are well established in the OECD Privacy Principles, national laws, ethical statements and codes of practice. Surveillance is defined as the systematic observation or recording of one or more people's behaviour, communications or personal information (Australian Privacy Charter Council, 1994). The use of technology for surveillance has three aspects:

a. Surveillance through information.
b. Surveillance of communications in cyberspace.
c. Mass surveillance using information and communication technologies.

Surveillance through information

One stop shopping and integration of data obtained by large entities, including government and commercial conglomerates, encourages merging of information provided for different purposes. Examples include marketing agreements like fly buy schemes and loyalty cards that offer discounts as rewards in return for details of purchases recorded to provide customer profiles. Efficiency benefits may flow from exchange of data and integration of databases but it is essential that the exchange of personal information takes place only with the informed consent of individuals. Individuals must have the option of continuing to deal separately with organizations and business units if they prefer. A key privacy principle is that information should generally not be used for purposes other than those for which it was collected (Australian Privacy Charter Council, 1994, Principle 15). Great care needs to be taken if information is used for secondary purposes (definitions used by various government agencies may differ and data provided by individuals may alter for legitimate reasons). Data-matching schemes have experienced a range of difficulties due to issues like data accuracy, integrity, administrative errors and much lower cost-benefit ratios than claimed at the outset.

Multimedia and convergence of new technologies allow unprecedented opportunities for invasion of individual privacy and surveillance of populations or target groups. When data items held in various formats are combined highly intrusive personal information is easily assembled and disseminated. Even if

informed consent is given each time personal data is collected by individual agencies it is unlikely that citizens will be fully informed about or aware of the detailed profiles that can be obtained from combined data (for example, linkages of visual images through photo licences, personal relationships through close circuit television (CCTV), and transactional data - non-anonymous payment of tolls and transport fares with computer records of addresses, health and financial data). Surveillance of individuals through the use of information is not compatible with human rights.

Surveillance of communications in cyberspace

Electronic communications can be monitored electronically using techniques and technology available in the public domain. Software programs can monitor and trigger recording of verbal and electronic communications. Powerful search engines allow Internet searches that monitor activities of individuals including those using news groups. Cookies (small pieces of data that a web server can store with a web browser) allow tracking of Internet users' visits to sites.

There is debate about the right of government and law enforcement agencies to intercept electronic communications and monitor Internet activities. Some enforcement agencies are concerned about the use of electronic money (ecash) and its potential for money laundering and tax evasion; others need to intercept communications among criminal groups. The need to balance law enforcement requirements with rights to privacy and freedom from surveillance is acknowledged, provided the response is commensurate with the level of risk to the community. Law enforcement agencies in most countries already have powers to tap telephone communications of individuals under certain conditions which are usually set out in law and clearly defined. Interception is usually justified during the process of obtaining a warrant or approval from an independent body. Monitoring private communications at random, or in accordance with pre-established automated triggers, is not conducive to freedom or democracy. Interferences with privacy must be justified.

There is debate about the responsibility of Internet service providers to monitor the content of material in cyberspace and to prevent certain transactions (for example, theft of data and risks to security) and transfer of unacceptable material (such as child pornography). It is argued that making Internet providers responsible for content is like making telephone service providers responsible for all voice and data carried on their networks. Will the Internet industry, as a whole, develop meaningful methods of self-regulation which clearly allocate responsibility for content? Will this be acceptable to all governments and to all citizens? A draft Internet Code of Practice prepared by the Internet Industry Association of Australia aims to establish general standards of behaviour for those involved in the Internet industry (Internet Industry Association of Australia, 1996, WWW).

Mass surveillance using information and communication technologies

Mass surveillance incorporates the concept of data capture and storage of information about citizens on a random basis. Mass surveillance creates a culture of fear among citizens. The use of information and communications technology for surveillance of individuals not involved in or suspected of illegal activities should

not be permitted. Satellite surveillance of citizens of sovereign countries without approval or justification can be considered as a form of invasion. Video cameras used in public areas without warning and storage of images of citizens obtained without justification should not be permitted. The growing use of CCTV in many countries on the grounds of providing security and protection against crime may tempt operators to store images just in case. Mass surveillance using techniques like automatic streaming through databases is very difficult to justify.

Principle 3: Citizens have the right to privacy and the right to conduct their affairs free from surveillance or fear of surveillance.

Freedom of Expression and Opinion

Cyberspace ignores national boundaries. 'Cyberspace is a place where the denizens are knowledgeable, independent and uppity. Found there is a new type of non-organization. ... cybertribes: like-minded citizens linked electronically by their key interest. They empower one another. They validate one another. Eager to find one another and communicate, they are also eager to influence real events ... (Draper, 1995, p. 30). It is important that cybertribes be permitted to develop. The concept of planet earth requires the free exchange of information, expression and opinion.

Individuals have a moral responsibility to be tolerant and honest in representing their personal views and the opinions of others (Merel, 1996, WWW). Ideally, honest political opinions should be expressed freely, without fear. But this may not be possible in all societies. For this reason the right to anonymous transactions is sometimes advocated particularly to protect whistle blowers and witnesses (Clarke, 1996, WWWa). Freedom of expression and free flow of information are required to support democracy and human rights. (Clarke, 1996, WWWa; Durango Declaration, 1995, WWW; Merel, 1996, WWW; Berleur and Brunnstein, 1996, p. 259). There is, however, a need to balance the right to freedom of expression with the responsibility not to cause harm to other citizens.

Principle 4: Cybercitizens have the right to freedom of expression and opinion and the responsibility to ensure the democratic rights and well-being of all citizens are protected.

Democracy

Cyberspace can be used to facilitate citizens involvement in the government of their own country and to influence world events. The ability to distribute material widely, cheaply and quickly allows issues to be discussed and feedback to be returned to the initiator swiftly. Information and communications technology can be used to facilitate participative democracy within nations and cyberspace. Electronic forms and computer analysis allow the responses of large numbers of citizens to be collated. The Durango Imperatives include calls for designers and applied research to develop infrastructure, architectures and technical interfaces that support democratic participation (Durango, 1995, WWW).

If governments and decision-makers are willing to share power and utilize the Internet to allow direct input by citizens or stakeholders a radical redistribution of power could occur. In the United States, '(a) national initiative and referendum movement already underway will allow people to bypass the Congress, to propose new laws and vote on them directly'. It is predicted that '(w)ith secure lines and positive electronic identification established, ultimately we will see on-line legislative initiatives and electronic voting, a return to direct democracy' (Draper, 1995, p. 730). It is particularly important in a period of significant change that policy development takes place 'in the highest level of participation and (that we) ... avoid the emergence of a two-tier society, (so that) ... the information society addresses the needs of citizens' (Laopodis and Fernandez, 1995, p. 2). Unlike television and mass media, cyberspace is interactive, provided there is no interference to prevent free access and distribution of information. Control of communications and media is frequently an aim of dictatorships. It is important that the unrestrained characteristics and complex matrices of the Internet are protected.

Principle 5: Cyberspace should be used to enhance opportunities for democracy within nations and across national boundaries.

Diversity of Culture and Ideology

Culture, defined as 'the way we shape our own destiny and make it understandable and practicable through all the institutions, rituals, means, etc., by which we regulate our violence' (Berleur, this volume) makes human thinking robust by providing options. Multiculturalism is a way of understanding, respecting and retaining cultural diversity. Cultural diversity is as important as biodiversity. Just as we need access to data from numerous sources to provide perspective and an opportunity to glean our truth, we need diversity in ways of thinking about events.

Technology usage is not neutral. Information and communication technologies can be used not only to control information about physical entities, including economically valuable objects and individuals, it can be used to influence thinking and behaviours. During the Gulf war dissemination/handling of news and access of the media to the military was very different to that during the Vietnam war. Monopolistic ownership and control of electronic information, cyberspace and the associated information and communications technology and infrastructure must be avoided.

Principle 6: Cyberspace should be used to support diversity of culture and ideology.

Equitable Distribution of Benefits

As in the industrial revolution, enormous shifts in economic benefit and distribution of wealth are occurring as the global information society emerges. Obvious impacts include workforce displacement, continued automation of information processing and manufacturing, and creation of a new elite with wealth and power based on ownership of electronic information and information and

communications technology and infrastructure. Our new high-tech economy has almost no need for unskilled workers and it is forcing de-massification of the labour force (Draper, 1995, p. 729). To prevent deskilling, equality of access to knowledge about information and communications technology must be available. The total time required from the human workforce to produce a specified quantity of goods and level of services has reduced. In many nations, some people labour longer hours while unemployment increases. Time savings, earning potential and opportunities for leisure need to be shared among all citizens so that wealth and quality of life can be distributed more evenly.

The industrial revolution led to enormous social upheaval in many countries. Social inequalities and denial of access to the benefits of industrial technology destabilized some societies and political systems. We must learn from history. The wealth and benefits of the global information society should be distributed equitably within and among nations.

Principle 7: All participants in the global information society, individual, corporate and government, should aim to distribute the wealth and benefits equitably.

Ownership of Data

Ownership of data in cyberspace relates to issues of copyright and intellectual property, rights to acquire, access and sell data about people, objects and transactions and transborder flows of data.

Copyright and intellectual property.

Ownership of copyright of electronic material and of intellectual property are issues of international concern being addressed currently. Protection and rights in cyberspace should be equivalent to those existing within the country of origin for non-electronic material, publications and broadcasts.

Rights to acquire, access and sell data about people, objects and transactions.

It is argued that computerized data owned by an organization belongs to that organization which has the right to sell or exchange that data, unless prohibited by law. The European Commission Directive related to the processing and movement of personal data (European Directive, 1995) will help protect European Community citizens in some circumstances but it does not address the issue of ownership rights internationally. Money is made from the sale of personal information despite the concern of individuals who believe their privacy has been invaded. If it was clearly stated in law that personal data is the property of the data subject, and this person has the sole right to permit an organization to use that data for authorized purposes, this trade in personal information would at least be reduced and at best cease.

Ownership of information about objects and transactions pertaining to a country is a vexed question. Burton summarizes the issue by asking whether information is a resource or commodity that can be bought and sold on the

international market. The treatment of information as a commodity derives from 'the high visibility of IT costs and the increasing degree to which information is created and manipulated by IT systems. ... Third world countries claim that information is a resource which can be used for development and that they have a right to control their individual information resources' (Burton, 1992, p. 59). Rights to acquire, access and sell data about objects and transactions within a nation should be determined by the laws of that country.

Transborder flows of non-personal data.

Transborder flows of non-personal data include:

- Operational data transmitted by multinationals for decision-making, financial purposes and administration.
- Data about a country, its economy, transactions and resources.

' ... Information transfer ... forms a significant part of all the international transactions taking place: it contributes considerably to the operational efficiency of multinationals and to export earnings ...' (Burton, 1992, p. 59). Some information held by private organizations is important to local national governments for understanding their economy. Who owns the data and who benefits?

National sovereignty and resource utilization are affected by transborder collection. (Who owns remotely sensed data relating to physical resources collected by satellite surveillance?) Third world countries argue that they need access to these databases and databanks located primarily in first world countries as a source of expertise and information for economic and social development. 'Systems are in place and are transferring and handling information on an international scale before third world governments (and some of those in the first world) have an opportunity to react: when they are able to consider policy, they are faced with entrenched situations and attitudes which are difficult to change, not least when these attitudes are held by multinational corporations backed overtly or covertly by national governments' (Burton, 1992, p. 58).

It is argued that data about the economy and resources of a country, and data originating in a country, are owned by that nation and continue to be subject to its law. Agreement about transborder collection and use of this data should be negotiated by the collecting/receiving nation or organization. Nations should have the right to access and use data about its economy and resources regardless of where it is stored.

Principle 8: Ownership of personal data resides with the data subject. Rights to acquire, access and sell data about objects and transactions within a nation should be determined by the laws of that country. Agreement about transborder collection and use of data about the natural, economic and social resources of a nation should be negotiated by the collecting/receiving nation or organization. Nations should have the right to access and use data about their economy and resources regardless of where it is stored.

CONCLUSIONS

The global information society is a threat to old social and economic patterns at local and international levels. Langdon Winner told the Durango Conference '... the move to computerize and digitize means that many pre-existing cultural forms have suddenly gone liquid, losing their former shape as they are retailored for computerized expression. As new patterns solidify, both useful artifacts and the texture of human relations that surround them are often much different from what existed previously' (Durango Declarations, 1996, WWW). And at the international level 'the clash between the real and the virtual realities is rendering ineffectual the edifice of national implementations of internationally agreed human rights' (Clarke, 1996, WWWa). The opportunity for reshaping inequitable, dysfunctional social and economic patterns has arrived. Faced with the power of information and communications technology and the political, economic, social and cultural impact of its use, a charter for citizens relevant to the global society and cyberspace is essential.

This charter for citizens of the global information society aims to promote the well-being of all citizens of all nations and of cyberspace. Its principles aim to establish the rights and responsibilities of all citizens and those using electronic information and cyberspace. Although these principles are only a beginning, each is designed to address a key issue arising from the global information society and cyberspace. They require debate, addition and refinement. But they are a beginning.

REFERENCES

Published documents

Australian Privacy Charter Council (1994), Australian Privacy Charter, *Australian Privacy Charter Council,* December 1994

Berleur, J. and Brunnstein, K., Eds (1996) *Ethics of Computing: Codes, Spaces for Discussion and Law*, A Handbook prepared by the IFIP Ethics Task Group, London: Chapman & Hall, 1996

Berleur, J. (this volume), Culture and democracy revisited in the global information society: Summary of a position paper

Berleur, J. (1996a), Final Remarks: Ethics, Self-Regulation and Democracy. *Ethics of Computing: Codes, Spaces for Discussion and Law,* Berleur, J. and Brunnstein, K., Eds (1996), *op. cit.,* pp. 241-253

Berleur, J. and d'Udekem-Gevers, M. (1996) Codes of Ethics Within IFIP and Other Computer Societies. *Ethics of Computing: Codes, Spaces for Discussion and Law,* Berleur, J. and Brunnstein, K., Eds (1996), *op. cit.,* pp. 3-15

Burton, P.F. (1992) *Information Technology & Society* Library Association Publishing, London, 1992

Cameron, J., Clarke, R., Davies, S., Jackson, A., Prentice, M., and Regan, B. (1992) Ethics, Vulnerability & Information Technology. *Information Processing 92 Vol. 11 Education and Society (ed. Aitken, R.) Proceedings of the IFIP 12th World Computer Congress* North Holland, 1992, pp. 344-350

Draper, M. (1995) Beyond Cyberspace: the Real Promise of Virtual Reality. *Vital Speeches of the Day* **61** (23) September 15, 1995, pp. 726-733

European Directive (1995) Directive 95/-/EC of the European Parliament and the Council On the Protection of Individuals with regard to the Processing of Personal Data and On the Free Movement of such Data. 2 February 1995

Laopodis, V. and Fernandez, F. (1995) Enhancing Citizens Participation in an Information Society, *5th Hellenic Conference on Informatics*, December 1995, published by the Greek Computer Society.

Nye, J. S. and Owens, W. A. (1996) America's Information Edge. *Foreign Affairs Journal* **75** (2) March/ April 1996, pp. 23-28

Electronic Sources - World Wide Web Sites and Email Contacts (as at 30 November 1996)

Benton Foundation (1996, WWW) United States Universal Service Provision www.benton.org

Clarke Roger (1996, WWWa) Speech to Victorian Council of Civil Liberties www.anu.edu/people/Roger.Clarke/II/VicCCL.html

Clarke Roger (1996, WWWb) NET-ETHIQUETTE: Mini case studies of dysfunctional human behaviour on the net www.anu.edu/people/Roger.Clarke/II/Netethiquettecases.html

Durango Declarations (1995, WWW) www.lanl.gov/SFC/95/declaration.html

Internet Industry Association of Australia (1996, WWW) Email:conduct@intiaa.asn.au, 1996

Kling, R. (1996) The Information Society: *Letter from Rob Kling for TIS*, **12** (1) Jan-May 1996. Email:kling@binky.ics.uci.edu

Merel, Peter (1996, WWW) The Expectations of Electronic Communities - *A Bill of Electronic Rights and Responsibilities, V0.15* www.usyd.edu.au/~pete/err.html

World Intellectual Property Organization Treaty (1996, WWW) www.public-domain.org/database/database. html

ACKNOWLEDGEMENTS

The authors acknowledge comments, contributions, and assistance from Roger Clarke, Diane Whitehouse, Patsy Segall, Margaret McEvoy, Graham Greenleaf, Philip Argy and Andrew Freeman.

The Charter for Citizens of the Global Information Society

This Charter assumes that all individuals of all societies have the rights set out in the United Nations Declaration of Human Rights. It aims to enhance the well-being of all citizens throughout the world. The objectives of the Charter are to reduce the vulnerability of individuals and societies, and to promote socially sustainable development of the Global Information Society. Exceptions to the Principles set out in this Charter must be justified, clearly stated, made in accordance with law, proportional to the necessities giving rise to the exception, and compatible with the requirement to enhance human rights.

Principle 1 - Individual and collective cybercitizens must protect the accuracy and integrity of digital information, adhere to all relevant ethical principles, codes and guidelines, and uphold the legitimate laws of nations.

Principle 2 - Nations should aim at equity of access to electronic information and cyberspace for all their citizens without discrimination.

Principle 3 - Citizens have the right to privacy and the right to conduct their affairs free from surveillance or fear of surveillance.

Principle 4 - Cybercitizens have the right to freedom of expression and opinion and the responsibility to ensure the democratic rights and well-being of all citizens are protected.

Principle 5 - Cyberspace should be used to enhance opportunities for democracy within nations and across national boundaries.

Principle 6 - Cyberspace should be used to support diversity of culture and ideology.

Principle 7 - All participants in the global information society, individual, corporate and government, should aim to distribute wealth and benefits equitably.

Principle 8 - Ownership of personal data resides with the data subject. Rights to acquire, access and sell data about objects and transactions within a nation should be determined by the laws of that country. Agreement about transborder collection and use of data about the natural, economic and social resources of a nation should be negotiated by the collecting/receiving nation or organization. Nations should have the right to access and use data about their economy and resources regardless of where it is stored.