0981

International Legal Notes

I A SHEARER

New OECD Guidelines for the Security of Information Systems

International Legal Notes

I A SHEARER

New OECD Guidelines for the Security of Information Systems

On 26 November 1992 the Council of the Organisation for Economic Co-operation and Development (OECD), meeting in Paris, adopted Guidelines for the Security of Information Systems. Australia is one of the 24 Member Countries of the OECD. The OECD comprises developed countries in Western Europe, North America, Japan and Australasia. As its title suggests, the focus of its concerns is economic. Much of its activity comprises the exchange and analysis of economic data. However, lately it has become more closely involved in social and legal consequences of the technologies which underpin modern economic development. Foremost amongst these is information technology. Social concerns presented by that technology have led to two initiatives by the OECD concerning the provision of normative guidelines to Member Countries on how to deal with particular problems. The first were the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*[1] Published in 1980, these Guidelines arose out of an Expert Group established by the OECD which was chaired by Justice Michael Kirby between 1978 and 1980.

The OECD Guidelines on Privacy proved highly influential in the development of Australia's laws on that topic. They were called to notice in this Journal soon after their adoption by the OECD Council.[2] Later they were adopted by the Australian Law Reform Commission as the core principles for the proposals of that Commission on Australian Federal legislative reform to protect privacy.[3] Subsequently, with some modification and development, the principles were incorporated in Pt III of the *Privacy Act* 1988 (Cth).[4]

In other OECD countries, the principles have likewise formed the basis of legislation on privacy protection.[5] They have also been adopted in the private sector, including by several multi-national corporations operating across national borders, as the basis of internal policy for the due protection of personal privacy in their data flows. It was the transborder feature of data flows and the difficulty of achieving satisfactory regulation of information systems by municipal law only, that led to attempts by inter-governmental agencies to produce effective protection for privacy. The Council of Europe developed two Conventions on the subject. But the OECD Guidelines, although not a formal binding treaty, have proved particularly influential in promoting consistent legislative treatment of privacy protection in OECD Member Countries. It was the reduction of the economic inefficiencies of disparate treatment of the subject of privacy protection which propelled the OECD into what was, for it, the novel activity of offering guidelines for the laws and practices of Member Countries.

Computer crimes and viruses

In the decade which followed the OECD Privacy Guidelines, it became clear that a number of additional but interrelated problems, presented by information technology, required inter-governmental attention. In particular, three issues continued to attract concern amongst major users of information technology. They were the reports of the steadily increasing incidence of computer-related crime, a new phenomenon of computer "hacking" and the introduction of highly damaging computer "viruses".

The OECD itself maintained, under one of its committees, a continuing scrutiny of the issue of computer crime. The economic significance of computer crime for societies increasingly dependent upon the reliability and accuracy of computer records, was obvious. Other international bodies also showed a lively interest in the topic. In 1989 the Committee of Ministers of the Council of Europe adopted a recommendation on computer-related crime. They urged moves to harmonisation of the law and practice of European countries on computer crime and for improved international legal co-operation to deal with such crime, wherever it had a transborder characteristic. Specifically, the report of the Council of Europe put forward a minimum list of subjects that should be covered by computer crime legislation (computer fraud; computer forgery; damage to computer data or programs; computer sabotage; unauthorised access; unauthorised interception; unauthorised reproduction of a protected program and unauthorised reproduction of topography). It also described an "optional list" of offences (alteration of computer data or programs; computer espionage; unauthorised use of a computer; and unauthorised use of a protected computer program).[6]

On a wider stage, the United Nations itself became involved in the issue of computer crime. In the Eighth United Nations' Congress on the Prevention of Crime and the Treatment of Offenders, held in Cuba in September 1990, a report was adopted affirming the need for the development of "appropriate international action" by Member States to "more effectively combat computer abuses that deserve the application of criminal sanctions".[7]

The problem of computer "hacking" and the introduction of viruses attracted widespread attention when it was shown, in the United States, that an offender, Mr Robert T Morris Jr, had introduced a "worm" into information systems with consequences involving financial losses to those affected estimated by the prosecution to amount to $US97 million. Mr Morris claimed an intention merely to show the vulnerability of the systems to intrusion. He was prosecuted and convicted under the *Computer Fraud and Abuse Act* 1986 (US). His conduct was illustrative of others whose viruses attracted such exotic names as "the Internet worm", "the Christmas tree virus", "the AIDS Trojan horse" and the "Italian bouncing ball virus". The "AIDS Trojan horse" involved an attempted extortion. Its perpetrator was arrested in Cleveland, United States, on a warrant issued in London from where most of the offending diskettes containing the virus were posted worldwide. As a consequence of these and similar acts, the Computer, Science and Telecommunications Board of the United States established a committee in 1990 to develop a national strategy on computer viruses. Its first recommendation was the promulgation of a comprehensive statement of generally accepted systems security principles.

There have been other national and subnational reports drawing to attention specific problems of computer crime, the vulnerability to intrusion, manipulation and distortion of many automated information systems. In Australia, the report in October 1992 of the Independent Commission Against Corruption (NSW), *Report on Unauthorised Release of Government Information*,[8] demonstrated a "shockingly widespread illicit trade in information held in the public sector". The trade operated between government officials, commercial firms and private inquiry agents. Information from Federal and State Government sources and the private sector was sold for private gain.

It is against the background of these developments that international initiatives, including those of the OECD, must be understood.

The OECD Expert Group on Security

In February 1990, in Toronto, Canada, an international meeting was organised, supported by a number of major international banks. International financial transactions are, potentially, specially vulnerable to intrusion, manipulation and crime affecting their transborder data flows. As a result of the Toronto meeting, a statement was issued by the participants urging renewed attention by the OECD to the issues of policy presented by the dangers to the security of information systems.[9] A number of the participants in the Toronto meeting (including the writer) had played a part in the OECD Expert Group on Privacy. Many were to participate in its forthcoming work on data security.[10] The result of the Toronto statement was a further impetus to the OECD to establish a new group on Security of Information Systems. The OECD had maintained a steady interest in security systems. In October 1988, one of its Committees approved preparation of a study on the subject of security of information systems. The result was a report, *Information Network Security* 1989. It was the review of this document which led the OECD Committee for Information, Computer and Communication Policy (ICCP) to convene the Expert Group which produced the Security Guidelines. This group had its first meeting at OECD Headquarters in Paris in January 1991. Justice Michael Kirby was in elected Chairman. Similar procedures were followed as in the earlier committee on Privacy. In a series of six meetings, the last in September 1992, Guidelines were produced for submission to the Committee for ICCP of the OECD and, if approved, to the OECD Council.

There was one feature of the second Expert Group on Data Security which distinguished it from the Privacy Group. A substantial contingent of experts from the private sector and from the trade unions participated in the discussions with the representatives and experts from the OECD Member Countries. As well, particular care was taken by the Secretariat officers in charge of the project (Dr H P. Gassmann and Ms Deborah Hurley) to consult widely with interested groups and to ensure that their comments on the Guidelines, as they were developed, were taken into account in the deliberations of the Group. Perhaps as a result of this, the Guidelines were quickly adopted both by the ICCP and by the OECD Council. The latter approved the Guidelines on 26 November 1992. They were recommended by the OECD Council for action by Member Countries.

Contents of the Guidelines on Security

In the statement issued following the adoption of the Guidelines, it was pointed out that information systems play an increasingly significant and pervasive role in national economies, international trade, government and business operations, health care, energy, transport, communications and education. The need for security for such systems required the protection of their availability, integrity and confidentiality. These three features of data security are well established.[11] According to the OECD statement:[12]

> "While growing use of information systems has generated many benefits, it has also shown up a widening gap between the need to protect systems and the degree of protection currently in place. Society has become very dependent on technologies that are not yet sufficiently dependable. All individuals and organisations have a need for proper information system operation (eg in hospitals, air traffic control and nuclear power plants). Users must have confidence that information systems will be available and operate as expected without unanticipated failures or problems. Otherwise the systems and their underlying technologies may not be used to their full potential and further growth and innovation may be inhibited."

The Security Guidelines now adopted by the OECD Council follow, in part, the pattern of the earlier Privacy Guidelines. They are accompanied by a recommendation to the Council of the OECD which recites the increasing use and value of information systems; the international nature and worldwide proliferation which has occurred; the growing inter-dependence of national and international economies as well as social, cultural and political life; the risks arising from inadequate safeguards; and the need to raise awareness of those risks and to respond appropriately to violations of security.

The recommendations of the OECD Council recognise that the Guidelines do not affect the sovereign rights of national governments on matters such as national security determined in accordance with national law. There is also a recognition (relevant to countries such as Australia, Canada, the United States and Germany) that, in Federal countries, observance of the Guidelines may be affected by the local constitutional division of powers. This said, the recommendations now adopted by the OECD Council recommend that Member Countries establish measures, practices and procedures to reflect the principles contained in the Guidelines; that they consult, co-ordinate and co-operate in their implementation; that they agree as expeditiously as possible on specific initiatives; and that they disseminate the principles of the Guidelines widely and review the Guidelines every five years with a view to improving international co-operation.

The Guidelines themselves are attached as an Annex to this note.

Accompanying the published Guidelines is an explanatory memorandum. It recites the earlier OECD initiatives. It then provides a textual commentary on the sparse language of the Guidelines as well as background information concerning the proposed scope of the problems of security of information systems to which the Guidelines are addressed.

It is now up to Member Countries of the OECD, and others, to consider the Guidelines and to commence the long process of bringing laws and practices into conformity, just as was earlier done following the adoption of the Privacy Guidelines.

Other initiatives on data law

It is worth noting that the OECD initiative on security of information systems has been running in parallel with other initiatives taken by other international bodies. One group which has been interested in issues of data security is the meeting of Data Protection Commissioners. Chaired by the Australian Privacy Commissioner (Mr Kevin O'Connor) that group held its first meeting in Australia in November 1992. Even more immediately influential is the current work of the Commission of the European Community. It has proposed a Council Directive on Data Protection.[13] In late 1990 such a directive was put forward in draft form. Further work on data security protection is also proceeding in the Council of Europe. The early completion by the OECD of its project seems likely to ensure that the OECD Guidelines are influential in shaping national and international laws and policies on this topic.

Australia was one of the last Member Countries of the OECD to accept the Privacy Guidelines. The delay followed the reference of those Guidelines to the Standing Committee of Federal and State Attorneys-General. The Privacy Guidelines were not finally accepted by Australia until 1983. The Federal legislation, after a false start when it became caught up with the Australia Card proposal, was not enacted until 1988. State legislation on privacy protection and extension of the Federal *Privacy Act* to other collections susceptible to Federal regulation remain for the future. It is possible that a response to the Guidelines on Security will come more promptly. The interest groups which support action tend to be banks, insurers and law enforcement bodies. They may enjoy greater governmental and legislative attention in Australia than the interest of groups which traditionally supported privacy laws. Time will tell.

References

[1] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Data Flows*, OECD, Paris, 1981. See D Korff, "International Data Protection" (1991) 6.4 *Interights Bulletin* 59.

[2] See M D Kirby, "The Computer, the Individual and the Law" (1981) 55 ALJ 443 at 448. See also (1991) 65 ALJ 354.

[3] Australian Law Reform Commission, *Privacy* (ALRC 22), 80 PS, Canberra, 1983, Vol 1, p 270.

[4] See s 14 (Information Privacy Principles).

[5] See, eg, *Personal Data Protection Act* 1988 (Japan).

[6] Council of Europe, European Committee on Crime Problems, *Computer-Related Crime*, Strasbourg, 1990, p 14.

[7] United Nations, 8th Congress on the Prevention of Crime and the Treatment of Offenders, *Report on the Prevention of Crime and Treatment of Offenders*, p 147 (A/Conf 144/28).

[8] See New South Wales (Australia), ICAC, *Report on Unauthorised Release of Government Information*, Sydney, 1992. See also A Roden, "Computer Crime and the Law" (1991) 15 Crim LJ 397. See also S Davies, *Big Brother: Australia's Growing Web of Surveillance*, Simon and Schuster, Australia, Sydney, 1992, p 100 and I Temby, "Australia Exposes Illegal Data Sales" (1993) 16 *Transnational Data Report* 26.

[9] M D Kirby, "Toronto Statement on the International Legal Vulnerability of Financial Information" (1991) 11 *Computer/Law Journal* 75. See also L J Hoffman (ed), *Rogue Programmes: Viruses, Worms and Trojan Horses*, Van Nostrand Reinhold, NY, 1990 and United States, National Research Council, *Computers at Risk*, National Academy Press, 1991.

[10] Including Mr R Buxton QC (UK); Professor M Horibe (Japan); Mr W List (UK); Mr Y Mine (Japan); Mr D Piragoff (Canada); and Professor B de Schutter (Belgium).

[11] But note that some experts suggest two further criteria of information security, viz "utility" and "availability". The OECD Expert Group did not accept these notions as central to the security idea.

[12] OECD, Press Statement, "OECD Adopts Guidelines for the Security of Information Systems", 27 November 1992 (92/86).

[13] European Communities, *Proposal by the Commission for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data* (COM [90]) 314, Brussels, September 1990.

MDK

ANNEXURE — pages 464-466

ANNEXURE

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

26 November 1992

I. AIMS

The Guidelines are intended:

- To raise awareness of risks to information systems and of the safeguards available to meet those risks;
- To create a general framework to assist those responsible, in the public and private sectors, for the development and implementation of coherent measures, practices and procedures for the security of information systems;
- To promote co-operation between the public and private sectors in the development and implementation of such measures, practices and procedures;
- To foster confidence in information systems and the manner in which they are provided and used;
- To facilitate development and use of information systems, nationally and internationally; and
- To promote international co-operation in achieving security of information systems.

II. SCOPE

The Guidelines are addressed to the public and private sectors.

The Guidelines apply to all information systems.

The Guidelines are capable of being supplemented by additional practices and procedures for the provision of the security of information systems.

III. DEFINITIONS

For the purposes of these Guidelines:

- "data" means a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means;
- "information" is the meaning assigned to data by means of conventions applied to that data;
- "information systems" means computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance;
- "availability" means the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner;
- "confidentiality" means the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner;
- "integrity" means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.

IV. SECURITY OBJECTIVE

The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.

V. PRINCIPLES

1. Accountability Principle

The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

2. Awareness Principle

In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

3. Ethics Principle

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

4. Multidisciplinary Principle

Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal.

5. Proportionality Principle

Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

6. Integration Principle

Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.

7. Timeliness Principle

Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of security of information systems.

8. Reassessment Principle

The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. Democracy Principle

The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

VI. IMPLEMENTATION

Governments, the public sector and the private sector should take steps to protect information systems and to provide for their security in accordance with the Principles of the Guidelines. In achieving the Security Objective and in implementing the Principles, they are urged, as appropriate, to establish and to encourage and support the establishment of legal, administrative, self-regulatory and other measures, practices, procedures and institutions for the security of information systems. Where provision has not already been made, they should, in particular:

Policy Development

—Adopt and encourage the adoption of appropriate policies, laws, decrees, rules, and international agreements, including provision for:

- harmonized worldwide technical standards, methods and codes of practice;
- promotion of expertise and best practice in the security of information systems;
- formation and validity of contracts and other documents created and executed in or by means of information systems;
- allocation of risks and liability for failures of the security of information systems;
- penal, administrative or other sanctions for misuse of information systems;
- jurisdictional competence of courts, including rules on extraterritorial jurisdiction, and administrative competence of other bodies;
- mutual assistance, extradition and other international co-operation in matters relating to the security of information systems; and
- means of obtaining evidence in information systems and the admissibility of such evidence in penal and non-penal legal and administrative proceedings.

Education and Training

- Promote awareness of the necessity for and the goals of security of information systems, including:
  - ethical conduct in the use of information systems; and
  - adoption of good security practices.
- Provide and foster education and training of:
  - developers, owners, providers and users of information systems;
  - specialists and auditors of information systems;
  - specialists and auditors of security of information systems; and
  - law enforcement authorities, investigators, attorneys and judges.

Enforcement and Redress

- Provide accessible and adequate means for the exercise and enforcement of rights arising from the implementation of the Guidelines and for recourse and redress for violations of those rights.
- Provide prompt assistance in procedural and investigative matters relating to breaches of security of information systems.

Exchange of Information

- Facilitate the exchange of information relating to the Guidelines and their implementation.
- Publish generally measures, practices and procedures established in observance of the Guidelines and for the security of information systems.

Co-operation

- On national and international levels, consult, co-ordinate and co-operate between and among governments and the private sector to encourage implementation of the Guidelines and to harmonize as completely as possible measures, practices and procedures for the security of information systems.