0966

AIC CONFERENCES

INFORMATION SECURITY MANAGEMENT CONFERENCE

Thursday 10 December 1992

OECD GUIDELINES FOR THE SECURITY OF COMPUTER STORED & TRANSMITTED INFORMATION

AIC CONFERENCES

INFORMATION SECURITY MANAGEMENT CONFERENCE

Thursday 10 December 1992

OECD GUIDELINES FOR THE SECURITY OF COMPUTER STORED & TRANSMITTED INFORMATION

The Hon Justice Michael Kirby AC CMG*

Chairman, OECD Expert Group on Security of Information Systems

WE ARE AT RISK

We are at risk. It is with these words that the United States National Research Council begins its recent report *Computers at Risk*.[1] The report goes on:

> *"Increasingly, America depends on computers. They control power delivery, communications, aviation and financial services. They are used to store vital information, from medical records to business plans, to criminal records. Although we trust them, they are vulnerable - to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. To date we have been remarkably lucky ... Unfortunately there is reason to believe that our luck will soon run out ... "*

The most difficult problem that faces that most fantastic engine of informatics - the human brain - is to see familiar

problems in a new light. It is to see the diamond from a different facet, after which it can never be perceived in the old way again. So it is in human affairs. We must see the issues of this conference from the perspective of the wider concerns in which provision of information security is but one illustration. The danger of modern existence is that, by so focusing our attention upon our immediate concerns, we are blinded to the context in which those concerns exist and to the deeper problems which they betray. The particular danger of technology is that it blinkers its specialists so that they perceive only the dazzling advances of their art and are impervious to the social fallout which the technology brings in its train.

Therefore, pause with me at the beginning of this contribution to consider the context in which the initiatives of the Organisation for Economic Cooperation and Development (OECD) in relation to information security must be evaluated. My thesis is that we are at risk indeed. But the fundamental risk derives from something far more basic, even, than the vulnerability of computers and information systems generally. It derives from the apparent incapacity of the international community and of the representative democratic process to keep pace with the social implications of technology.

Consider the great forces which are at work in our world today. They have been described by various shorthand expressions. One tension is between global fusion and local fission. It is between the globalisation which is inspired by the modern technological revolution and the tribalisation of humanity which infects the attitudes of individuals and

groups to the issues of their political regulation and government. At the one moment in history, therefore, the world with its wizardry of technology pulls in one direction whilst the mind of humanity seems to be shrinking and turning back to the narrow focus of ancient enmities and local parochialism. There are exceptions of course. Many busy international institutions and armies of civil servants respond to the phenomenon of globalism. The United Nations Organisation itself. The Council of Europe. The European Communities. And their institutions. The Secretariat of the [British] Commonwealth of Nations. But there are difficulties both at the international, national and local levels of government and administration. We do no service to human affairs by ignoring these difficulties. Indeed the imperative of modern technology, which is such a force for change in our time, requires of us that we should seek out and institute the global arrangements necessary to respond to the issues presented by technology and (in so doing) to defend basic human values.

IMPEDIMENTS TO INTERNATIONAL HARMONISATION

As mine is a contribution about the intercontinental institutional response to the subject matter of this conference, let me start by acknowledging some of the impediments which stand in the way of a truly effective international response to the issues of information security. These impediments will be well known to you all. They are certainly recognised by the Expert Group of the OECD which I had the honour to chair. They include:

1. Whilst the technology of informatics is universal, the

institutions for social regulation of problems such as data security, remain resolutely national or even local;

2. Whilst there have been many moves towards international institutions to serve the global community of the 20th century, such global institutions have tended to be weak and vulnerable to strongly felt national and local concerns. The economically weak may be noisy in the institutions of the world. But, when the chips are down, it is the economically and politically powerful who will generally make the vital decisions. They will usually do so by reference to their perceived national interests. Altruism is rare. True internationalism is exceptional. This is understood by all players;

3. The international institutions engage a parade of visiting politicians and bureaucrats. They, in turn, are served by contingents of civil servants striving to accommodate often conflicting instructions and (not unreasonably) to assure their own survival. The larger and more diverse the institution, the more numerous and contradictory will be the interests to which the participants give voice. At one recent international agency (WHO) I was reminded that the average duration in office of a minister in a developing country is less than a year. Thus the drama of international agencies is played out by a huge team of constantly changing actors, of greatly varying capacity and interest, usually with large egos and, sadly, often with little real commitment to the substantive international business which is temporarily in their charge;

4. Back home the political leaders must respond to increasingly pervasive democratic pressures. We hear much loose talk today of the triumph of democracy over autocracy in the world. Yet the reality falls sadly short of these proud boasts. Political leaders are, all too often, chosen not by the people, or even their elected representatives, but by powerful vested interests. They are beholden to those interests which, in turn, are hapless captives of the necessity to raise funds for their political parties. Election campaigns are waged in terms of grossly superficial slogans. Image has all too often replaced substance. This is itself, in part, a product of the information technology of mass communications. It is in this way, that the "democratic revolution" is increasingly debased. The kinds of players who are interested in that particular game are, all too often, uninterested in the tedious business of dealing with complex technological, economic and sociological phenomena;

5. Instead, the political process, both nationally and internationally, is frequently responsive to passing fads and fancies, to prejudice and local, parochial concerns. There are occasions when the world holds its breath as important issues of principle are asserted and upheld. Kuwait was an example. Perhaps Somalia and Macedonia are others. But these are truly exceptional events. For the most part the political leaders of our nations have little if any international vision. The very political process which spawns them domestically usually contracts their minds to

provincial concerns. Not for them the urgencies of responding to the global necessities of effective international data protection law and policy. Much more likely is it that they will respond to the passions of old, ethnic and cultural tribalism which is such a feature of our world today and in which some votes may be found;

6. If initiatives can be stimulated in an international agency to deal with a global problem such as information security, the pace is all too often glacial. In part, this is an inescapable function of the costs of bringing together representatives of many nations . In part, it reflects the wholly proper obligation to consult the numerous departments, agencies and interests back home before offering a commitment to any global approach. In part, it may reflect constitutional obligations. The history of this century was profoundly affected by that requirement of the United States Constitution which obliges the President to have the advice and consent of the Senate to the ratification of treaties;[2]

7. There is also the curtain of our many languages and cultures through which we must deal with each other in resolving problems which are global in character. I pass over the obvious fact that words in different languages may not mean exactly the same thing. Nuances of meaning, inherent in the different history and experiences of the many communities of the world, impact upon the way in which the self-same text can connote quite different ideas to readers approaching

its common language from the perspective of their different world experience. The institutions of the international community which we share today were largely conceived and put in place after 1945 by countries which at least shared the European cultural tradition. Inevitably, therefore, those institutions reflect the Judeo-Christian values of the West. It is probably also fair to say that they are especially influenced by the value systems of the Anglo-American powers, victorious in the War and most influential in the institutional arrangements which followed it. We may talk of *human* rights. We may accept a *universal* declaration of such rights. We may labour within the framework of the international agencies which bear the stamp of the old Anglophone power. But these universals have not necessarily kept pace with the changing character of the world's politics and economics since 1945. In Australia, a much discussed book, *The Confucian Renaissance*,[3] has recently pointed to the dichotomy between the character of our international institutions and the growing power of the Confucian societies of North Asia. According to the authors, these countries (including China and Japan) are content for the moment to work within the global institutions. Necessarily, reflecting as they do their own differing cultural perspectives, they regard some aspects of the present global institutions as alien. These are to be tolerated for the moment. But they will come to explain less and less of the reality of international

arrangements.[4] That reality is likely, increasingly, to move into the realm of informal arrangements which may even run quite contrary to publicly expressed notions of international intercourse. It is essential, for occidental members of the international community striving to find global solutions to the inter-connected problems presented by common technology, to acquaint themselves with the different perspectives which may exist in the cultures of societies like China and Japan, which do not necessarily share all of the assumptions implicit in Western values. What is true of Confucian societies will also have its equivalents in the societies of the Islamic world and of parts of Africa, Central and Latin America and the Malay communities and the peoples of the Pacific and Oceania. The time has arrived when negotiators in international *fora* from Western countries must instruct themselves in the differing values and approaches of people of different cultural traditions. Finding common positions on controversial issues in the world as it really is, requires nothing less; and

8. Finally, there is the impediment familiar to us all. Once there was talk of two nations: the rich and poor of any country. That dichotomy still exists. Recent events may have even exacerbated it. But now it also finds its reflection *between* nations. It presents itself in a new aspect: the technologically rich and the technologically poor. We see this between states and within communities. Relevantly to institutional

responses to common problems, we see it in the different cultures of the technologist (on the one hand) and the lawyer/administrator (on the other). Too often these groups think in different ways and talk past each other, understanding only part of what each is saying. The dazzling complexity of modern technology leaves many bureaucrats and lawyers bemused, even intimidated. There is, occasionally, a sense of despair that the subject matter of proposed regulation will ever be understood. If understood, the chances are that the target will move before the snail-pace procedures of regulation are set in train, let alone adopted. Whilst talking, consulting and refining are the typical techniques of the lawyer and policy-maker, the technology bounds ahead. Language chosen to respond to one form of technology is soon perceived as inadequate (or even inappropriate) when a change in the technology renders carefully crafted words inadequate, inappropriate or even positively obstructive.

A CASE OF MELANCHOLY FAILURE

I have taken these pains to outline the critical features of the world we live because they are relevant to the task of developing an international régime to respond to the vulnerability of information systems. There will be many in this audience, and beyond, who will consider the need for international regulation (or at least "rules of the road") to be so self-evident and urgent as to feel a sharp sense of impatience at a lawyer's protest about the difficulties of achieving that end. A recent Japanese publication put it well:[5]:

"The development of network technology has enabled mutual connection of information systems across national borders, creating a borderless society in information processing. As a result, it is now possible to access any part of the world in the same amount of time, a social framework everyone acknowledges to be very efficient and convenient. On the other hand, the consequences of failures in information systems increase in proportion to the degree of network expansion. For this reason social stability cannot be maintained in an age of global information unless all countries uniformly adopt the same level of minimum security measures. ... [T]he influence of security problems occurring in less protected systems can now extend even to sufficiently protected systems if they are connected via networks. This means that weak parts need to be eliminated from the whole. Today, actions taken locally can have only limited effectiveness in the field of information system security. We have now reached a junction when all countries must collaborate in the study of information security in the global age."

To all of that I would say amen. It is simple and self-evident. It is urgent and necessary. Indeed, the establishment of an effective international régime on security of information systems is seriously overdue if one takes into account the enormous expansion of network technology which has already occurred.[6] So what is holding things up?

I have listed some of the main political, institutional and cultural impediments. We must have these clearly in our minds in order to understand the minefield through which we are treading. It is an obstacle course, far more complex even than the labyrinthine processes of achieving policy consensus and legal regulation within our own several political systems. If, therefore, we accept the challenge of this meeting (as I believe we must) we should have the obstacles to success clearly in our sights. And we should

learn from the difficulties which have resulted in the failure to achieve international regulation in equivalent areas where globalisation of technology seems equally to call out for regulation.

Two recent conferences which I have attended have concerned not security but an analogous problem of international regulation: the liability of air carriers for losses occasioned to passengers and cargo. Soon after the advent of civil aviation, shortly after the First World War, the government of France set in train steps designed to achieve an international agreement which would provide a common global régime on this topic of air carrier liability. The negotiations ensued from 1923 until the Warsaw Convention was signed in 1929. It was a Convention which was aimed at laying down a uniform system for the recovery of compensation. The need for such a system was obvious. Most people would not easily be in a position to prove fault on the part of an air carrier in the case of loss or accident. They (or their survivors) would often live in different countries. In an international activity, an international system was essential.

To some extent the Warsaw System has been a success. More than 160 countries have ratified the Convention. It provides for the recovery of amounts fixed by the Convention, without proof of fault. The limits on the sum recoverable could be circumvented if wilful recklessness on the part of the air carrier can be demonstrated. But the basic problem is that the system, extremely cautious to begin with, has totally failed to keep pace with inflation and the exponential expansion of international civil aviation. The

Warsaw Convention fixes a "cap" on recovery expressed in terms of gold francs. There is some uncertainty as to what this now discarded unit of value means. But most people accept that the value fixed for death or injury is only about $US11,000. So grossly inadequate is this sum in today's world that seemingly endless efforts have been made to negotiate revisions which will delete the reference to gold francs and increase the amount of the "cap" fixed by the international treaty. One would have thought that this endeavour would have been seen as a self-evident international necessity. But 62 years, further Conventions and five Protocols later, the international régime, as such, has not been properly reformed.

Various countries have adopted amendments to the Convention. The United States' Senate is considering a proposal of President Bush to ratify two amending Protocols. Under seven successive United States Presidents, starting with President Eisenhower, attempts have been made to get reforms through the Senate. The stumbling-block has been the perception that the no-fault compensation provided by the international revisions was inadequate by United States standards. The result has been an international legal régime which is a "shambles". Some international airlines (such as QANTAS and Japan Airlines) have voluntarily increased their liability. To avoid the risk of the United States withdrawal from the Warsaw System altogether, all airlines flying into and out of the United States must accept higher levels of compensation. People can take out private insurance (although few do). If a levy of $1 or $2 on every air ticket were raised, a completely satisfactory international régime

could be put in place. But for more than 40 years, our international system has been talking about reform. It has failed to achieve what is patently necessary. There is no uniform system. The precise amount of compensation recoverable after an accident is uncertain. Compensation payouts are delayed. There is no proper régime for renewal and updating of the system which is in place.

Think about these gross inadequacies when next you are at a crowded airport. Look at the vast hordes of humanity moved about by the wide-bodied jets, to the great benefit of peace and commerce in the world. What a tragedy it is that the lawyers and regulators so hopelessly fail to keep up with the leaps of imagination of the scientists and technologists. So grossly inadequate now is the limit of the Warsaw Convention that people who suffer loss to passengers and cargo are virtually forced to sue in the courts, seeking to circumvent the limit by proving wilful recklessness. But the result of this (and of the failure of the international community to do what is obviously required) is that:

* Fifteen years after the Pam-Am accident in Bali in 1974 no recovery has been achieved by the families of those killed;
* Eight years after the Korean Airlines disaster over the Soviet Union, not a penny has been paid to the families of United States passengers seeking to break the limitation; and
* Three years after the Lockerbie disaster in Scotland, the families are still waiting. Meanwhile mortgages have had to be paid and childrens' college education accounted for.

We, who are charged with devising international institutional responses to the problems of information security, should learn from this melancholy tale of failure in an analogous field where a rapidly expanding new technology presented the international community of nation states with an urgent necessity to find common rules. In information security we should strive to do better.

A CASE OF NOTABLE SUCCESS

We can do better in the field of data security and in a sense we must. Urgent as the provision of a just international régime for air liability is, the necessity of a compatible international régime for security of information systems appears even more urgent. The interactions are even more pervasive. The ramifications reach even more directly into the lives of virtually every one of us. You do not have to travel to be caught up in the problem, although if you do, you are. The perils of loss and damage to life and property are even greater than in air mishaps. We have survived all these years with a hotch-potch of improvisations in air liability rules. It is unlikely that we will get by for much longer without an appropriate, agreed international régime on the security of general information networks.

There is a glimmer of hope. It arises from the comparative success of earlier international endeavours to provide guidelines on a related aspect of the social implications of informatics. I refer to the work of the OECD on the Guidelines on Privacy.[7] I can speak with some knowledge of that enterprise. Between 1978 and 1980 I chaired the Expert Group of the OECD which produced the

Guidelines on Privacy. Those Guidelines, in the form of a recommendation by the Council of the OECD, was adopted and became effective in September 1980. The Guidelines have proved most useful in the development of laws and policies in a number of OECD countries, including Japan and Australia.

It is important to remember that the OECD's exercise on privacy did not commence in a vacuum. The *Universal Declaration of Human Rights* had included, in Article 12, a provision that:

> *"No one shall be subjected to arbitrary interference with his privacy ... Everyone has the right to the protection of law against such interference or attacks."*[8]

This principle was picked by the *European Convention on Human Rights* and by the *International Covenant on Civil and Political Rights*.[9] With the advent of computers, a new problem was presented for privacy or (as it is now often called) data protection and data security. First, a number of the Scandinavian countries separately, then the Nordic Council and later the Council of Europe, produced drafts which sought to isolate the basic principles of privacy protection in the computer age. The principles became refined. They reflected a largely chronological approach to the movement of data through a system. They governed the collection of the data, quality of the data once collected, the use of the data, the security applicable to the data, the rights of the individuals and others affected to have access to the data, in part to ensure compliance with the earlier principles. The Council of Europe developed conventions which were open to member countries of the Council of Europe. However, useful as the principles

collected in those conventions were, they tended to be European in orientation and to reflect machinery provisions which were not always congenial to a number of states outside Europe.

The choice then faced by the international community was a familiar one: fusion or fission. Fusion on the one hand would suggest the sharpening of explicit legal obligations within the smaller subgroups of the communities principally affected, such as the European Community (EC). Indeed, directives are presently under consideration which, in explicit ways, will enlarge the obligations of member countries of the EC for the protection of privacy. The alternative path was to spread the basic, minimum principles to a wider world. UNESCO and the United Nations system generally exhibited interest in privacy protection. Although some claimed that privacy was a luxury of developed societies, others pointed out that basic human rights were universal and as important to persons in Africa and Asia affected as to those in Europe and North America.

However, distracted by other concerns, UNESCO and the UN system were less effective in pursuing this issue than the OECD proved to be. It is a body of intercontinental membership. It collects the principal developed countries of the world. It spans the hemispheres: extending from Europe and North America to Japan, Australia and New Zealand in the Pacific. Reaching consensus within the OECD on the value-loaded issue of privacy protection was a much greater challenge than achieving a similar objective within Europe, with its largely shared traditions and common economic interests.

Various tensions emerged within the original OECD Group. The Europeans, with fresh memories of the misuse of personal data by the secret police of European dictators were perhaps more alert to the practical dangers against which safeguards were needed. The Anglophone countries, led by the United States, were perhaps more sympathetic to the importance of free expression and the free-flow of ideas. The economic interests of the Americans reinforced their philosophical convictions. Their representatives often expressed concern that controls for privacy protection were actually disguised efforts of some European countries designed to protect local information technology industries rather than human values in privacy.

Notwithstanding these and other differences, agreement was finally struck. The Council of the OECD recommended to member countries that they should take into account in their domestic legislation the principles contained in the Guidelines. It also recommended that they should endeavour to avoid creating: -

> ... *in the name of privacy protection, unjustified obstacles to transborder flows of personal data.*"

The most influential part of the Guidelines on Privacy is Part 2, being "Basic Principles of National Application". It is this part which has influenced a great deal of domestic policy-making and law-making. That is precisely what the OECD Committee and the Council had in mind. To the extent that different countries went about the regulation of inter-active data flows in different ways, it was clear that such regulation would be totally ineffective, inefficient or

such that no participant in the data flows could possibly comply, at the one time, with the differing procedural and substantive obligations of all régimes affecting such flows.

Such incompatibilities and inconsistencies would be economically disruptive and legally confusing. As well, their existence would diminish the effectiveness of the protection of rights to privacy. Thus it was the very international dimension of the technology which necessitated the preparation of the OECD Guidelines. Those Guidelines were deliberately non-coercive in form. They did not envisage a binding treaty, such as the Warsaw Convention. The hope was that, by getting the basic principles right, we would lay down a system which, by good example, would permeate the laws and policies of member countries of the OECD. In this way consistent and compatible rules would be developed which would reduce the inefficiencies of divergent approaches, diminish the confusion and result in better international and national protection of the value of privacy.

In Australia, the OECD Guidelines have been adopted, at federal level, by the *Privacy Act* 1989. That Act applies to specified information systems under federal regulation, such as in the Federal Public Service and credit reporting agencies. Australia was rather slow in acceding to the OECD Guidelines on Privacy because of the consultations with the States which were thought to be necessary. Under the Australian Constitution, the States share certain law-making responsibilities with respect to privacy concerns. Those consultations took some years. The Federal Government's first effort to implement the Guidelines was linked to a

proposal to establish a universal identification card, with the engaging name of the *"Australia Card"*. Defeat of that legislation in the Australian Senate actually caused a Double Dissolution of the Australian Federal Parliament. When the Government was returned, the legislation was re-presented. However, subsequently it was abandoned when huge public protests belatedly developed, about the proposed universal identifier card. In Australia no-one has to carry a passport or ID card. It was then that the Government proceeded with the separate privacy legislation. That legislation contained "Information Privacy Principles". They are expressly set out in the Australian *Privacy* Act. They follow very substantially the OECD Guidelines.

A not dissimilar development occurred in other countries, such as Japan. The word "privacy" was rarely used in Japan, at least before the latter half of the 1950s.[11] No precise translation of the concept, from its development in Anglo-American law and other Western law, could readily be achieved into the Japanese language. However, in terms of legal process, the idea gained attention after 1964 following a novel by Yukio Mishima concerning the private life of a political candidate.[12] By the 1970s, calls were being made for effective legal protection. A Personal Data Protection Bill was introduced into the Diet in March 1975 by the Opposition. But no legislation was introduced by the Government and none was enacted. In August 1980, by which time the OECD Guidelines were completed and awaiting approval by the Council of the OECD, Professor Horibe wrote a book *The Contemporary Privacy*.[13]. In it he proposed legislation, both nationally and locally in

Japan, on the model of the OECD Guidelines. He has expressed the view that:

> *"The recommendation of this international organisation had great impact on the Japanese government."*

Japan was one of the first countries to subscribe to the OECD Guidelines. In January 1981, the Administrative Management Agency set up a study committee. It produced a report in July 1982. That report proposed five fundamental principles for privacy protection, obviously derived from the OECD Guidelines. There was no immediate legislative action at the national level, although some local governments enacted ordinances on the model of the report.[14] As in Australia, so in Japan. The national government, beset with many other problems, took a great deal of time to consider the proposal for privacy legislation. A further study group was established. In Australia too we have committees to report on the work of earlier committees. Eventually, however, a Bill was produced in April 1988. This was approved by both Houses of the Diet. The *Personal Data Protection Act* 1988 came into force on 1 October 1989. The Act provided for a further delay in the introduction of the facility for disclosure and correction of personal data.

During Diet deliberations of the Bill, attention was drawn to the neglect of the regulation of privacy in the private sector. The Government gave a commitment that it would advance promptly its investigations in that regard. The Ministry for International Trade and Industry (MITI) in April 1989 issued a document setting out guidance on personal data, notably in consumer credit.[15] MITI adopted

policies calling on industry associations to investigate the implications of Guidelines on privacy in the private sector. Professor Horibe comments that:

> *"The MITI policy will play a very important role ... because MITI implemented the Report of the Personal Data Protection Subcommittee by issuing circular notices ... and promulgating the 'Rule on the Register concerning the Measures etc for the Protection of Computer Processed Personal Data' in the Official Gazette on July 7, 1989."*[16]

In addition to the foregoing, guidelines have been published in Japan on personal data in financial institutions and on the protection of such data in local government. Each is also based on the OECD Guidelines.[17]

The result of the foregoing is a very clear demonstration of the "ripple effect" of the OECD Privacy Guidelines in Japan as in Australia. The course taken is, in fact, largely the same. Careful national deliberation and widespread consultation. Eventual legislation regulating the national public sector. Later specific provisions in relation to credit reference systems. Now there are moves to extend the principles into the information systems of the private sector but to do so, at least at first, by guidelines rather than justiciable, sanctioned legal regulation.

I believe that this is exactly what the OECD Council and the Expert Group on Privacy had in mind. It was to give a common intellectual framework to the policy and lawmakers of member countries, such as Australia and Japan. By doing so, it was hoped that common principles would be accepted and inefficient discordancies avoided. In the case of Australia, Japan and other countries it is a hope that is being realised. It illustrates what can be done in the field of

inevitable. In 1986, the OECD issued an analysis of legal policy on computer related crime.[22] It contained guidelines for national legislatures. It was specifically related to the international character of many computer related offences. It suggested common denominators for the approaches that should be taken.

Similar steps were also under consideration in the Commission of the European Communities.[23] Eventually the Council of Europe's Committee on Crime Problems published the results of its research. In a report issued in 1990, it laid out what it described as Guidelines for National Legislatures, being a "minimum list"[24] and an "optional list" of data offences which should be covered by local law.[25] Most helpfully, the report contained a review of the initiatives of a number of national legislatures, including the United Kingdom, the United States and Canada. It also contained an analysis of the particular problems presented by the international aspects of computer related criminality involving transfrontier activities. The report concluded:

> *"Computer-related criminality involving a transfrontier situation is becoming increasingly important. Because of the nature of computers, there is an increasing potential for storing, moving, using and manipulating data by contact from long range, and the ability to communicate and to transmit rapidly large quantities of data between computer systems over a long distance. ... The offence may be committed partly in one jurisdiction and partly in another, or even partly in a third one, initiated from practically any place in the world. Obstacles such as distance, border control or necessity of physical presence are no longer relevant."*[26]

This report catalogues the new problems presented by

challenges of this kind. They include the inadequacy of the territorial principle and the need to achieve extra-territorial jurisdiction; the need for harmonisation of substantive criminal law; and the problem of "direct penetration" of information systems. The need for important changes in substantive and procedural law to cope with penetration of into systems was clearly established.

Because the problems identified in these and many other reports were clearly of a global, and not simply a European, character, suggestions came to be made concerning the way in which harmonisation on a wider scale could be achieved beyond the frontiers of Western Europe. Certain initiatives could be taken by the Commonwealth Secretariat for member countries sharing the history of British rule. But, more relevantly to the use of informatics in the United States and Japan, a new international vehicle was necessary.

At a forum on the vulnerability of international financial information held in Toronto, Canada in February 1990, a concluding statement by the participants urged new initiatives at an international level. The trigger for a new-found sense of urgency were the many reports of serious harm caused by the manipulation of information systems:

> *"Sometimes with fraudulent intent, sometimes without intent to secure personal gain but with reckless indifference to the consequences of the conduct involved."*[27]

The report of the forum recorded the new problem of invasions of information systems by viruses with arresting names such as "internet worm", "world peace virus", "the Jerusalem virus", the "AIDS Trojan horse", the "Italian bouncing ball virus" etc.[28] This new problem and the serious

substantive and practical difficulties of tackling issues of data security on an international scale led to a call for new initiatives at the international level:

> *"Already cases of damage to innocent users of information technology systems have been prosecuted in the courts. The possibility of significant increases in such cases must be faced squarely. Laws, security practices and investigative techniques must be improved to deter would-be offenders, to detect those who offend, to secure their conviction and punishment and to provide for fair apportionment of liability for the losses which occur from their actions and from error in the process. Whilst action on the level of individual jurisdictions is proceeding in all of the countries represented at the forum, at different levels of detail and different speeds, and whilst some international cooperation has been achieved (notably in UNCITRIAL ... OECD, the Council of Europe, etc) there is no international agency with a specific mission to examine and advise on the harmonisation of laws and practices in all of regions represented."*[29]

It was in this environment that the Toronto forum called for action:

> *"[B]ecause of its intercontinental membership and activities, its economic mission and its proved track record in facilitating international consensus on principles relating to information technology and transborder data flows, the OECD seemed to some participants to be a suitable venue for the further exploration of some of the computer offence-related concerns of this forum."*

Perhaps stimulated by this vote of confidence, the Committee for Information, Computer and Communications Policy (ICCP) of the OECD eventually established an *ad hoc* Group of Experts to prepare Guidelines for the Security of Information Systems. That Group held its first meeting at OECD headquarters in Paris in January 1991. I was elected Chairman. Its secretary was Dr Hans Peter Gassmann. Its

principal secretariat officer was Mrs Deborah Hurley. The Group had six meetings, the last of which was held in September 1992. Those Guidelines were adopted by the Council of the OECD on 26 November 1992.

OECD's MISSION IN THE NEW WORLD ECONOMIC ORDER

This initiative of the OECD must be judged in the context of the overall strategy and mission of that Organisation in the current world economic and political ferment. That mission was most recently expressed in the *Communique* issued by the Council of the OECD on 5 June 1991. That Council Meeting was attended by the senior Ministers of the 24 member countries of the Organisation. The Ministers reasserted:

> *"The basic values shared by the OECD countries ... pluralistic democracy, respect for human rights and market oriented economies."*[30]

The Ministers stressed:

> *"The need for OECD and non-Member countries alike to formulate coherent policies in the fields of economics, environment, social affairs and technology that are mutually reinforcing in support of broadly based sustainable development."*[31]

As a top priority for strengthening international economic cooperation they called for:

> *"... close policy cooperation [to] help to provide a sound global economic environment".*[32]

They called on the Organisation to:

> *"... develop and deepen its work on structural issues and, where appropriate ... in those issues which lie beyond the ambit of current*

international negotiations, consider the feasibility of elaborating operational arrangements."[33]

Specifically, in the field of technology the Ministers noted that it would increasingly underpin national economic performance providing a:

> *"... need for governments better to coordinate and ensure coherence amongst domestic policies in these fields."*[34]

In the annex to their statement, the Ministers recognised the potential for increased international friction arising from differences in national policies. They concluded:

> *"... with a view to reducing divergencies which cause frictions in these policy areas, Ministers ask the OECD, where appropriate, to explore the need for improving existing multilateral instruments and whether there is a need to develop additional 'rules of the game'."*[35]

The work of the Expert Group on Security of Information Systems must therefore be understood in this context. The Group derives legitimacy not just from the delegation of the ICCP Committee which set it up. But also from the overall strategy of the Ministerial Council of the OECD at a time of rapid economic and political change in the world.

The OECD is not alone in its endeavours on information security. In the field of data protection, the Council of the European Communities has established a Working Party on Data Protection. The latest report of that Working Party concerns a meeting held on 21 June 1991.[36] The Working Party is steering towards an action plan designed to develop an EC strategic framework for the security of information systems. The object is to identify user requirements, the

needs of suppliers and service providers and to develop standardisation, evaluation and certification and technological and operational advances in the security of information systems.[37] It is stated that this action plan should complement:

> *"... evolving European and international standardisation activities in this field."*[38]

Many of the participants in the EC exercise also take part in the work of the OECD Group. That Group is likewise aware of the activities taken within the Government of the United States to secure common national standards in that country for computer and communications security.[39] So far, work within the United States governmental agencies has been related largely to the protection of national security or to meeting one major element of security, viz confidentiality. But the National Research Council report, referred to above, acknowledges that United States programmes:

> *"... have paid little attention to the other two major computer security requirements, integrity (guarding against improper data modification and/or destruction) and availability (enabling timely use of systems and the data they hold." These requirements are important to government system users, and they are particularly and increasingly important to users of commercial systems. Needed is guidance that is more wide-reaching and flexible than that offered by the so-called Orange Book published by the National Security Agency, and it should be guidance that stimulates the production of more robust trustworthy systems at all levels of production."*[40]

Accompanying these international, transnational and national developments have been initiatives of governmental agencies and academic scholars designed to isolate, in a

theoretical and practical way, the basic objectives to be achieved for security and the means of securing them.

One of the most important of the practical analyses studied at the recent meeting of the OECD experts was that adopted by MITI as its Computer Systems Security Standards. These standards do not, as such, have legal force in Japan. But according to a review of them they:

> *"... could serve as a basis for procurement of IT product systems by government organs or corporations."*

The point made by the analyses of such Japanese standards is that measures taken for the security of information systems to date have largely concentrated on protection against loss or damage caused by natural disasters and by systems structures. The rate of computer-related crime in Japan is low. Perhaps for that reason, security awareness of systems managers is described as generally low. The object of the MITI standards is to improve knowledge, to encourage a proper conceptualisation of the issue and to meet new challenges, such as those presented by computer viruses.

The first security standards were laid down by MITI in 1977. They have been revised in 1984 and again in 1991. As well as the general standards of MITI, there are particular standards laid down in Japan by the Ministry of Posts and Telecommunications, the National Police Agency, the Ministry of Autonomy and other bodies. But the MITI standards are of the greatest general importance. They are organised into facility standards, technical standards and operating standards. They are put forward substantially to stimulate action which will prevent breaches of security. Obviously,

prevention is preferable to the *ex post* provision of punishment of offenders or remedies for those who suffer loss. However, ultimately, the law will have to provide for such criminal and civil redress. As such, it cannot be provided by Guidelines declared nationally, still less internationally. In Japan, to deal with the illegal behaviour which arises from computer-aided offences, criminal and other laws were partly revised and enacted from June 1987.[41] Such reforms provide for punishment in the case of illegal production and destruction of electromagnetic records; wilful disruption of a another party's business through electronic means; and property crimes. Such crimes are defined to include the illegal acquisition of profit by providing false data or illegal commands to a computer to produce forged records regarding the acquisition of, or change of, property rights or by providing the described forged data for a third party's clerical use. Two proposed crimes were excluded from this amendment to Japanese law and left for future study. They were:

* Illegal acquisition and/or transfer of data processed and stored by computers; and
* Unauthorised use of a computer.

THE OECD GUIDELINES

The OECD Guidelines on Security follow significantly the format of the successful Privacy Guidelines. I annex the Guidelines to the text of this paper. They are accompanied by a substantial explanatory memorandum to elaborate their particular provisions. They are preceded by a number of recitals which briefly elaborate the necessity of an

international approach to this issue. They include recommendations that steps be taken nationally to reflect the principles promulgated in them and internationally to secure harmonisation of the applicable rules.

The core information security principles, which lie at the heart of the Guidelines) are surrounded by a list of applicable definitions and a charter of steps that will be necessary to implement the Guidelines, according to the legal and administrative cultures of the several countries of the OECD, if their objectives are to be attained.

The information security principles are grounded, as most earlier studies on the subject are, upon the need to ensure that the information system respects the three identified chief components of information security. These are:

* *Availability*, ie that the applicable data is present, accessible or attainable and immediately capable of use for a purpose by persons authorised to access it;
* *Confidentiality*, ie that the data should not be made available or disclosed to persons who are unauthorised to have access to such data; and
* *Integrity*, ie that the data once accessed has not been altered or destroyed in any unauthorised manner.

This tripartite division of the concept of security in the context of information systems is very well established in the literature.[42] More recently, however, a number of writers have suggested that there are, in fact, further aspects which must be incorporated into an effective

information security system. A further two criteria suggested by one notable expert are said to be:

* *Authenticity*, ie assuring the genuineness of the data; and
* *Utility*, ie its usefulness once accessed.[43]

I do not overlook the fact that future developments will certainly expand the understanding of the notions of information security with the passage of time and the development of new technological possibilities.

Four further core "principles" are accepted in the new OECD Guidelines. These are:

* The *awareness* principle: ie that means should be readily available for those entitled to be informed about the existence and extent of the measures which have been put in place for the security of information systems. This is fundamental so that a person whose data is stored in the system can elect whether the security provided for the protection of values such as confidentiality and privacy (not to say intellectual property and other rights) are adequate for that person's purposes;
* The *proportionality* principle, ie that the measures for security should be proportionate to the degree of reliance on the data and the magnitude, possibility and implications of any breaches of security. No completely secure system can be devised. Even the best encryption codes can usually be broken. The greatest perils are those of human error and failure. The measures put in place should be proportional to the

needs for security. Such measures should keep in mind issues such as cost effectiveness. An undue obsession with security for its own sake should be avoided;

* The *free-flow* principle, ie it is essential, in free societies, to realise that measures for secrecy, restriction and security are necessarily in competition with the free-flow of information. The legitimate entitlement of the community and of other individuals to the benefits of free-flow must be balanced against the claims of the government, corporations and individuals to the enforcement of data security; and
* The *accountability* principle, ie that there should be an identifiable person who is responsible for the enforcement of the applicable security principles and accountable for derogations from them.

Many other issues are under consideration for inclusion in the Guidelines. They include:

* The desirability of promoting international harmonisation of technical, administrative and other standards;
* The need clearly to allocate risks and liability;
* The need to provide for jurisdictional competence in multi-jurisdictional cases;
* The need to provide for mutual assistance and improvement of extradition laws for transborder crimes; and
* The need to provide penal measures for deliberate or reckless interference in information systems.

In addition to the consultations within the OECD Group,

informal consultations took place within national administrations and with national experts so that the final product would be the best that could be produced in the present state of the technological art and of the perception of the problems which need to be addressed. The experience with the OECD Privacy Guidelines demonstrates how influential such international guidelines can be for domestic law and policy-making.

CONCLUSIONS

There is a need for a greater sense of urgency about the provision of effective measures for the protection of the security of all information systems, but especially of those stored, processed, retrieved or transmitted by information technology. If the security of such systems is only as strong as their weakest links, it will be insufficient for each nation merely to embark upon its own national laws and policies for information security.

Truly, we live in the age of globalisation. It is the challenge of the coming generation to rescue the intellect and attitudes of humanity from the narrow parochialism of the past. Nothing less will do when the technology which has sprung from the mind of man presents international problems which urgently demand international solutions.

The OECD has, in the past, provided an important contribution to the development of law and policy relevant to the age of informatics. It is my hope, and expectation, that the work of the Expert Group on Information Systems will enjoy similar success. I commend the Guidelines on Security of Information Systems to Australia law-makers and systems-users.

FOOTNOTES

* President of the Court of Appeal, Sydney, Australia (1984-). Chairman, OECD Expert Group on Transborder Data Barriers and the Protection of Privacy (1978-80). Chairman, OECD Expert Group on Security of Information Systems (1991-92). Governor, International Council for Computer Communications (1984-). Member, the Tide 2000 Club. Personal views.

1. United States, National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, 1991, 7.
2. United States Constitution, Article II, s 2. The reference is to the rejection of the League of Nations. See also below.
3. R Little and W Reed, *The Confucian Renaissance*, Federation, Sydney, 1989.
4. *Ibid*, 99.
5. Japan Information Processing Development Center, Final Announcement of Symposium, 3.
6. See eg the special issue of *Scientific American* ("Communications, Computers and Networks") September 1991, esp, V G Cerf, "Networks", *ibid*, 72.
7. Organisation for Economic Cooperation & Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris, 1981.
8. *Universal Declaration of Human Rights*, art 12.
9. See arts 8 and 17 respectively.

10. Masao Horibe, *Access to Information Held by the State and Privacy in Japan*, Paper for the XIII International Congress of Comparative Law, Montreal, August 1990, *mimeo*.

11. *Ibid*, 15.

12. The plaintiff recovered most of the requested damages of Y800,000 in the Tokyo District Court. See Horibe, *ibid*, 15.

13. *Id*, 17.

14. *Id*, 19.

15. *Id*, 22.

16. *Loc cit*.

17. *Id*.

18. Council of Europe, European Committee on Crime Problems, *Computer-Related Crime*, Strasbourg, 1990, 14.

19. *Ibid*, 15.

20. *Id*, 16.

21. *Id*, 17.

22. Organisation for Economic Cooperation and Development, ICCP Report No 10, *Computer-related Crime: Analysis of Legal Policy*, Paris, 1986.

23. See Council decision, 26 July 1988; O J No C 288, 21 October 1988.

24. Council of Europe Report, *op cit*, 36.

25. *Ibid*, 60.

26. *Id*, 83.

27. See M D Kirby, "Toronto Statement on the International Legal Vulnerability of Financial Information", [1990-91] 3 *Computer Law and Security Report*, 2, 3.

28. *Ibid.* See also L J Hoffman (ed) *Rogue Programs: Viruses, Worms and Trojan Horses*, Van Nostrand Reinhold, New York, 1990, 61ff;

29. [1990-91] 3 CLSR 2.

30. Organisation for Economic Cooperation and Development, Press Release (SG/Press (91)(31)) Paris, 5 June 1991, 1.

31. *Id*, 2.

32. *Id*, 4.

33. *Id*, 4.

34. *Id*, 7.

35. *Id*, 20.

36. European Communities, Council, Working Party on Economic Questions (Data Protection), Outcome of Proceedings, Brussels, *mimeo*, 29 July 1991.

37. *Ibid*, 2.

38. *Id*, 3.

39. National Council Report, above n 1, 3.

40. *Id*, 3.

41. *Current State of Computer Security-Related Policies and Measures*, a document provided by the delegation of Japan to the OECD Expert Group, 7.

42. See International Standards Organisation (ISO), "Security Architecture", Part II in *Information Processing Systems: Open System Interconnection: Basic Reference Model* ISO-7498-2 available from the American National Standards Institute, New York, 1989.

43. Cf D B Parker, "Restating the Foundation of Information Security", confidential note (Applied Research Note 11 - Revised).

Annex to the Recommendation of the Council
of _____, 199_

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS

(_____, 199_)

I. AIMS

1. The Guidelines are intended:

a) To raise awareness of risks to information systems and of the safeguards available to meet those risks;

b) 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;

c) To promote co-operation between the public and private sectors in the development and implementation of such measures, practices and procedures;

d) To foster confidence in information systems and the manner in which they are provided and used;

e) To facilitate development and use of information systems, nationally and internationally; and

f) To promote international co-operation in achieving security of information systems.

II. SCOPE

2. The Guidelines are addressed to the public and private sectors.

3. The Guidelines apply to all information systems.

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

III. DEFINITIONS

5. For the purposes of these Guidelines:

a) "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;

b) "information" is the meaning assigned to data by means of conventions applied to that data;

c) "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;

d) "availability" means the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner;

e) "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;

f) "integrity" means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.

IV. SECURITY OBJECTIVE

6. 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

Accountability Principle

7. 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.

Awareness Principle

8. 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.

Ethics Principle

9. 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.

Multidisciplinary Principle

10. 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.

Proportionality Principle

11. 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.

Integration Principle

12. 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.

Timeliness Principle

13. 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.

Reassessment Principle

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

Democracy Principle

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

VI. IMPLEMENTATION

16. 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

a) 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

b) 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.

c) 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

d) 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.

e) Provide prompt assistance in procedural and investigative matters relating to breaches of security of information systems.

Exchange of Information

f) Facilitate the exchange of information relating to the Guidelines and their implementation.

g) Publish generally measures, practices and procedures established in observance of the Guidelines and for the security of information systems.

Co-operation

h) 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.