UIC John Marshall Journal of Information Technology & Privacy Law

Volume 11
Issue 1 *Computer/Law Journal - Winter 1991*

Article 4

Winter 1991

Toronto Statement on the International Legal Vulnerability of Financial Information, 11 Computer L.J. 75 (1991)

Michael Kirby

TORONTO STATEMENT ON THE INTERNATIONAL LEGAL VULNERABILITY OF FINANCIAL INFORMATION

*The Hon. Justice Michael Kirby, A.C., C.M.G.**

I. INTRODUCTION

Information systems and international networks have grown rapidly in scope and complexity over the last decade and have created certain novel vulnerabilities. An international forum of experts met in Toronto, Canada between 26 and 28 February 1990 to consider current issues of international legal vulnerability of financial information.

The participants discussed:

- The allocation of responsibility when an error or loss occurs in an international information system;
- Legal implications of recent computer "hacking," systems viruses and other threats to the integrity and security of computer networks;
- The current state of national and sub-national laws to deal with such offenses;
- The procedural and resource difficulties faced by police and others in tracing the perpetrators of such offenses; and
- The growing need to secure international cooperation in developing the appropriate laws and practices to deal with such offenses.

The participants noted the effective systems and safeguards which have been set in place by many institutions to deter, prevent and detect offenses connected with their information systems and to secure the evidence necessary to bring those guilty of offenses before courts for trial and, if convicted, punishment. They recognized the legitimate role of alternatives to purely legal solutions to many of the problems discussed.

The participants noted the steps being taken in some jurisdictions to establish by law sensible rules for the apportionment of civil liability

* Companion of the Order of Australia; President, Court of Appeal, Supreme Court of New South Wales, Australia; Chairman, OECD Expert Group on Transborder Data Barriers and the Protection of Privacy (1978-80); Governor, International Council for Computer Communications (1984-); Commissioner, International Commission of Jurists (1984-).

in money transfers in such a way as to fairly distribute losses where they occur as a result of computer related errors and offenses. They commend to their own governments the urgent study of such initiatives, both national and international. In the opinion of the participants a greater sense of urgency in the provision of such laws and policies is needed.

International challenges require international solutions. Cases having a connection with a number of different jurisdictions demonstrated the frequent difficulty, or even impossibility, of applying laws in force in one jurisdiction to a problem connected with several. Conflicts in the obligation of obedience to inconsistent court orders have arisen in different countries. Significant discrepancies in the definitions of offenses in different countries exist. Existing forms of international cooperation in criminal investigation, such as extradition or mutual assistance seem not always adequate. Extradition of offenders is not always possible. Tracing the source of international hacking is difficult.

The antisocial dimensions of computer hacking and computer viruses must be brought home to the public which still tends, all too frequently, to glamorize the harmful activities of hackers and computer frauds. Society increasingly relies on the integrity of information systems. It is the duty of society to protect and assure that integrity.

The international character of the phenomena necessitates the development of an appropriate forum for the exchange of information, the drafting of guidelines and the preparation, in due course, of appropriate international law. The participants recognized the value of work already under way and attention being given, in such organizations as the OECD, UNCITRAL, the Council of Europe and the UN Committee on Crime Prevention and Treatment of Offenders and urged more immediate attention to encouraging all countries to pass legislation that will cover new risks arising through new forms of computer misuse, and in particular, to the needs for international cooperation in dealing with the international nature of these issues.

II. SUMMARY RECORD

Meeting in Toronto

1. Between 26 and 28 February, 1990 a group of invited experts met in Toronto, Canada to discuss aspects of the international legal vulnerability of financial information. The meeting was sponsored by the organizations listed in Annexure A. It was organized by Dr. Peter Robinson (Canada) and Mrs. Anne Branscomb (U.S.). The names of the participants are set out in Annexure A. The participants took part in the meeting and expressed views in their personal capacities.

2. The participants came from Western Europe, North America,

Japan and Australia. They represented diverse backgrounds, including judges, lawyers in private practice, academics, government and bank lawyers, bankers, fraud investigators, computer security experts and police. Participants stressed the importance of increasing public awareness about the realities of computer related offenses and reducing the hype, glamour and romanticism that often misguidedly accompanies media representations of the issues. They authorized the release of this Summary Record of their discussions to interested bodies and individuals. Necessarily, the summary can record only some of the many diverse points discussed during the two and a half day meeting. As befits participants from different linguistic, cultural, and legal environments and free societies, diverse opinions were expressed. This extended to the perceptions and definitions of the issues, the solutions that should be offered to meet those issues, and the institutions in which such solutions might best be developed.

International Technology, International Problems

3. Nevertheless, there was consensus upon one obvious and simple matter; that the developments of information technology, with its instantaneous multi-jurisdictional characteristics and its potential for virtually instantaneous transactions, present new and puzzling problems for the legal order, the banking and finance industry, and commerce in general. Cases of damage to innocent users of information technology systems have already 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 (notable in UNCITRAL, The Organization for Economic Cooperation and Development (OECD), the Council of Europe, etc.), there is no international agency with a specific mission to examine and advise on harmonization of laws and practices of all of the regions represented.

4. With an international technology come interjurisdictional problems — of law, detection, policing, civil liability, and criminal punishment. There is therefore a need for a higher degree of international cooperation in this area than has been achieved to date. The cooperation necessarily includes:

- greater collection and exchange of information about the nature and

dimension of the problem of offenses related to interjurisdictional movements of financial information;
- enlarged cooperation between police and other related investigative agencies in different jurisdictions concerned in the investigation and detection of such offenses;
- increased cooperation between law enforcement and prosecutorial authorities in different jurisdictions and revision of treaties and laws on extradition to ensure that some jurisdiction will have authority to redress at least those acts commonly deemed harmful; and ideally, that offenders are brought to justice in the most appropriate jurisdiction with regard to their acts;
- improved cooperation between banks and other financial institutions and common carriers of data to improve arrangements and techniques designed to identify would-be offenders and prevent them from succeeding in their endeavors; and
- accelerated cooperation on an interjurisdictional basis in the exchange of data and expertise, the provision of guidelines on harmonization of laws and practices and the possible eventual development, in selected areas, of reciprocal and internationally enforceable laws on criminal and civil liability for defined offenses and civil wrongs connected with international exchange of financial information.

Additional resources and better training for personnel of investigative organizations may be required.

Structure of the Meeting

5. The forum agenda was divided into a consideration of the following topics:
- SUBSTANTIVE LAW: with a consideration of the current state of criminal and civil law and the provision of a number of perspectives from organizations from around the world.
- PROCEDURAL LAW: with a study of problems of collecting admissible evidence for the proof of offenses, the need to secure public cooperation and the deglamorizing of computer "hacking"; the identification of a number of priority issues from the perspective of policing and the gathering of data for the more precise definition of legal and policy targets for action.
- INTERNATIONAL COOPERATION: with the examination of both the need for, and measure of cooperation achieved in, harmonization of laws related to information technology offenses. This session examined the processes of harmonization both of substantive criminal and civil law and of procedural law. In this session there was also discussion of the present and future work of international agencies in this field, notably UNCITRAL, the Council of Europe, the ITU, and the OECD.
- ALTERNATIVE APPROACHES: with an examination of means of supplementing or substituting for purely legal solutions to the issues addressed during the forum. Amongst alternatives examined in this

session were the introduction of codes of conduct and the heightening of public awareness and education about the antisocial and even life threatening, dangerous, and destructive features of some information technology offenses. Professional ethics, police and investigative training, and enhancement of practical international cooperation were also discussed in this session.

- THE FUTURE: in the final session the participants turned to a consideration of future trends. The agenda of the forum is Annexure B to this Summary Record.

Substantive Law Issues

6. The discussion of substantive law issues included a study of a number of recent instances of information systems manipulation, sometimes with fraudulent intent, sometimes without intent, to secure personal gain with reckless indifference to the consequences of the conduct involved. The cases mentioned — not all of which directly involved financial information — were described under the typically exotic names by which they have become known, such as:

- "Internet Worm"
- "World peace virus"
- "Christmas tree virus"
- "The Jerusalem virus"
- "The AIDS trojan horse"
- "The Italian bouncing ball virus"
- "The Morris Worm" etc.

7. In some cases, offenders have been prosecuted for criminal offenses. Some convictions have been secured, including a notable conviction for computer "hacking" under the *Computer Fraud and Abuse Act* (U.S.) of Robert T. Morris, Jr. (awaiting sentence at the time of the forum), who was found to have introduced a worm into information systems with consequences involving financial losses to those affected estimated by the prosecution to amount to U.S. $97 million. Mr. Morris's defence was that he believed, when he introduced his "worm" into the affected systems, that it would not have such a major impact so quickly but would merely show the vulnerability of the system to intrusion. These and similar cases bring to light the ambivalence in some quarters about appropriate social attitudes to such activities. Some observers condone the activities of a brilliant student who demonstrates the inadequacy of computer security protecting data. Others regard the conduct as seriously antisocial and call for deterrent punishments and civil liability laws to make intrusions less attractive and to spread the burden of the losses incurred.

8. Just as serious as the Morris case was the much publicized distribution, late in 1989, of thousands of personal computer diskettes ostensibly with data about the AIDS virus. These diskettes contained,

instead, a very serious "trojan horse" which disabled information systems into which they were inserted, allegedly for the purpose of extracting an extortion for the retrieval of otherwise lost data. The alleged perpetrator of this offense has recently been arrested in Cleveland (U.S.) on a warrant issued in London, England, from where most of the diskettes were posted worldwide (but not to the U.S. and Canada). The diskettes were allegedly distributed from a Panama registered company. The case awaits trial. Although it does not directly involve interference in international financial information, it neatly illustrates the legal complexities and the interjurisdictional character of many information offenses today.

9. Various classifications of information technology offenses have been proposed both by national and international agencies. Different jurisdictions have adopted different expressions of offenses. Some have opted for a conceptual approach with a comprehensive new code of computer related offenses. Others, particularly countries of the common law, have preferred a piecemeal approach: legislating particular new offenses. Some have adopted precise definitions, e.g., of "computer", "data", "information", etc. Others have preferred to leave offenses expressed in very general terms to take account of the continually changing terminology and the inadvisability of adopting laws which may soon be rendered out of date by the rapid advances in information technology which have been such a feature of the past two decades. The participants recognized that there is tension between:

- the clear expression, in simple language, of conduct which can be stigmatized as antisocial and punished but which is not expressed in terms dependent on a particular technology; and
- the definition of criminal offenses with a precision of language which recognizes the derogation from liberty involved in creating new crimes.

10. The participants noted that international agencies have attempted to assist the harmonization of domestic law by providing a minimum and an optional list of offenses. For example, the Council of Europe *Guidelines* provide the following list of offenses which are defined in general terms:

A. *Minimum list*:

1. Computer fraud;
2. Computer forgery;
3. Damage to Computer Data or Programs;
4. Computer Sabotage;
5. Unauthorized Access;
6. Unauthorized Interception;
7. Unauthorized Reproduction of a Protected Computer Program;
8. Unauthorized Reproduction of Topography.

B. *Optional list*:

9. Alteration of Computer Data or Programs;
10. Computer Espionage;
11. Unauthorized Use of a Computer; and
12. Unauthorized Use of a Protected Computer Program.

11. The varying extent to which countries already provide criminal offenses apt to the above-described conduct, the disparity of the present expression of such offenses, and the even greater diversity of laws on the assignment of civil liability for losses were noted in the context of the multijurisdictional character of issues. The particular difficulties raised by the diversity of laws and conflicts between differing laws in differing jurisdictions was illustrated by reference to a number of cases. Typical of these were two cases involving Hong Kong and the United States. In one of these, a major English banker with branches in the United States and Hong Kong was ordered by a United States court to comply with an order for the production of banking information on a Hong Kong customer who had allegedly breached laws in the United States. The customer secured an injunction from the Hong Kong courts protecting its banking privacy. The bank drew this injunction to the attention of the court in the United States, but to no avail. It was fined heavily for each day that it was in contempt of the U.S. court order. The U.S. contempt orders were drawn to the attention of the Hong Kong courts but again to no avail. It was reported that the proceedings were settled in a way permitting the bank to purge its contempt. But the case, and several others involving Canadian and other banks illustrate the occasional difficulty, in the absence of international law or comity between courts of different jurisdictions, in complying with differing laws affecting the same parties and the demands for and protection of information. It also reflects the interest which governments and courts have in access to information relevant to their various functions.

12. Amongst other points made in this session were:

- The need to educate prosecutors who, even many years after the enactment of new specific offenses, often prefer to prosecute under old general offenses which pre-date new information technology;

- The need to express new substantive offenses in terms which can be explained, in the case of jury trials, to ordinary citizens in a way that makes the antisocial nature of the offense sufficiently clear;
- The need for legislatures to face up to hard choices in the provision of new criminal offenses, aided by expert bodies, law reform agencies, and internationally approved guidelines;
- The need to keep the cost of security in balance with its utility was stressed by many participants, as was the need to provide a graduated scale for the protection of data of differing sensitivity and value;
- The need to provide a balance between the social and economic desire for the free movement of information and the protection of confidentiality. This balance may be struck differently depending on the type of information involved. Comprehensive legislative schemes to achieve these balances may be required;
- The possible need to look again at the civil liability of common carriers and agencies that provide telecommunication services. As such bodies offer a greater range of services and move away from being mere conduits for communications, the arguments for removing or reducing their immunity from civil liability increases in a system of law designed to spread and share the risk of the inescapable factor of loss involved in transnational offenses; and
- The need to provide appropriate fora for the discussion of reasonable security standards.

13. A number of participants who investigate computer related offenses emphasized that the reluctance to disclose computer offenses as they occur is counterproductive:

- It masks the true dimension of the social problem;
- It reduces the pressure on the legislature and government authorities to address the problem, including the provision of adequate resources and properly trained and adequately paid investigators; and
- It diminishes the public realization of the unacceptable social cost of such activity.

The experience of one major United Kingdom bank was described. The bank decided to give publicity to the activities of a "hacker" who had secured unauthorized entry into the bank's financial records. The bank's actions and security policies were publicly explained. The results were support for the introduction of remedial legislation into the UK House of Commons, much public commendation for the bank's actions and openness, a contribution by the bank to public education, and no reported loss of customer confidence. There was discussion among the participants about the possible need for laws or practices requiring reporting in defined instances of information fraud affecting financial information. On the other hand, the participant recognized that there was sometimes a need in public trials to protect security systems and confidential information.

14. Although much of the session on substantive law concerned

the provision of new criminal offenses (for deterrence of wrongdoing and the conviction and punishment of wrongdoers) the participants also considered schemes for the risk allocation and assignment of liability for losses involved in errors and offenses concerning commercial electronic funds transfers, including those having an international character. The various solutions adopted, e.g., agreements between customers and institutions, institutions and other institutions or by bilateral or multilateral treatises were considered. The model law on liability for commercial funds transfers proposed for adoption by the American Law Institute and the National Conference of Commissioners on Uniform State Laws of the United States of America as a possible model for a national law to govern the respective rights and liabilities of "financial institutions" and the "sender of a payment order" was considered. *See* new Article 4A Funds Transfer of the *Uniform Commercial Code* (U.S.). The participants discussed comparative advantages of legal rules which encourage appropriate levels of security for financial data on the part of banking and financial institutions whilst adequately protecting users who may sometimes be less readily able to absorb losses. A number of participants decided that their national governments should encourage UNCITRAL to move more expeditiously to develop principles for risk allocation in commercial electronic funds transfers.

Procedural Law Issues

15. The participants next examined the legal and practical procedures that were necessary to any effective detection, control, and redress of offenses related to financial information. A number of participants with a background in policing and fraud investigation brought home some of the practical problems involved. These included:

- The need for pooling intelligence on incidents and losses in order to disclose patterns of fraudulent transactions by "repeat players";
- The need for heightened cooperation in police and other training, including in specialized colleges in other jurisdictions;
- The need to recruit, and pay at an appropriate level, highly skilled police and other investigators to assist in the detection and prosecution of such offenders;
- The need to secure cooperation between common carriers and agencies providing telecommunications services and police, and if necessary changes to the law, to permit under appropriate condition of confidentiality the monitoring of electronic transactions to detect "hackers" and other persons engaged in information offenses;
- The need to enhance formal and informal cooperation between law enforcement and like agencies across jurisdictional borders; and
- The need to reform the law to enhance in precise ways the powers of investigation agencies to cope with the new problems presented by interjurisdictional offenses.

16. One problem of law enforcement peculiar to computerized international financial information is the very short time typically available to an investigative agency to freeze the information evidence before it is transmitted out of the jurisdiction. The need to provide an internationally acceptable, reciprocal power to law enforcement agencies, when alerted to a possible offense, was discussed. But participants stressed:

- The commensurate need to ensure respect for the sovereignty of other legal jurisdictions;
- The need to protect legitimate customer rights to unimpeded international flows of information;
- The need to avoid reliance on subterfuge or informal arrangements between agencies, otherwise than in compliance with the law; and
- The need to avoid unduly enlarging official intrusion into personal and corporate privacy and confidentiality for the sake of preventing occasional loss.

Nevertheless, several participants expressed the opinion that a suitable remedy for freezing such transactions for a short time could be designed with appropriate legal safeguards. The unsuitability of most slow-moving prosecution machinery presently available was recognized but so were the differing attitudes of various states to changes in this connection.

17. There was considerable discussion of the laws of evidence and the requirements of due process. It was recognized that whilst these laws sometimes frustrate law enforcement and investigative bodies, and even sometimes thereby occasion loss to innocent third parties, they often involve fundamental constitutional guarantees or are accepted as the price paid for controlling the great power of the state and protecting natural justice and basic civil liberties. This means, as was recognized by the participants, that the price to society of detecting and punishing all cases of offenses related to information systems would be too high if it involved departures from such fundamental principles.

International Cooperation

18. The third session examined the problem presented to the international legal order by the advent of information technology, which by its nature is largely indifferent to jurisdictional borders. The special problem that criminal law is typically defined in terms of the jurisdiction's sovereign control over its own territory was considered as were various solutions which have been adopted or proposed to deal with information offenses having a transnational character. These include:

- The passage of long-arm statutes with (purported) effective extraterritorial operation of one state's law in another legal jurisdiction;
- The negotiation of extradition treaties between more countries and

the return of accused persons for trial on a wider range of offenses on new principles of mutuality and reciprocity;
- The enlargement of formal and informal exchanges between law enforcement and like agencies;
- The establishment of an appropriate international legal regime to facilitate telecommunication interception and tracing to combat and detect information network offenses;
- The negotiation of bilateral treaties to deal with particular offenses;
- The reductions of disparity of laws by compliance, in domestic lawmaking, with internationally devised guidelines leading to the harmonization of the expression of offenses; and
- The consideration of multilateral treaties for particularly heinous crimes. Such treaties exist for crimes of an international character such as terrorism against diplomats, attacks against civilian aircraft and some drug trafficking offenses. The possible future development of international law on at least some informational crimes having a transnational character was discussed.

19. The participants recognized the slow processes involved in developing, adopting, ratifying, and (in some cases) enacting such laws domestically. Nevertheless, the initiatives taken by UNCITRAL, OECD and the Council of Europe and the potential of other international agencies such as the International Telecommunications Union (ITU), the Secretariat of the Commonwealth, the International Chamber of Commerce, or the UN Congress on Prevention of Crime and the Treatment of Offenders to play a part in relation to informational crimes were recognized by the participants. An international problem eventually demands international cooperation and solutions. It was recognized that, apart from the problems of delay inherent in international negotiations, other difficulties exist; including differing legal cultures and traditions and the likelihood that some regions of the world will not be covered by such regimes, at least in the short run. Nevertheless, the participants acknowledged the need to begin and recognized that inaction was unacceptable give the present size and likely future growth of the problem.

20. The work of the committees of OECD, the Council of Europe and UNCITRAL were particularly noted as especially valuable. The potential for activity by United Nations agencies was recognized as important because virtually all countries participate in U.N. bodies. Each international organization has a valuable role to play in addressing the various issues raised. Some agencies may have more appropriate resources to address particular issues than others. There is a need for bodies to focus their work on particular aspects of the problem. However, because 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 trans-

border data flows, the OECD seemed to some participants to be a suitable venue for the further exploration of some of the computer offense related concerns of this forum. Other bodies, such as the upcoming UN Congress on Crime Prevention and Treatment of Offenders should also be encouraged to give attention to these matters. UNCITRAL was recognized as the agency currently developing risk allocation rules for commercial electronic funds transfers.

Preventive Law and Alternative Approaches

21. In the fourth session the participants considered alternatives to strictly legal approaches to offences and civil liability. The emerging trend towards professionalism in some aspects of information processing was noted. The participants noted that this professionalism could potentially reinforce legal sanctions and proper conduct and discourage abuse by operatives. In this regard accreditation of colleges and universities which did not discourage unauthorized "hacking" into computer systems was questioned. The possibility of licensing some key workers in information processing was mentioned, but was recognized as controversial. The role of industry codes of conduct and of research into standards of performance by operatives was examined. The role of raising public awareness in order to change occasionally indulgent community attitudes to information crimes was explored. Such changes were recognized as necessary preconditions to stimulating informed public appreciation of information network crime and to securing the proper allocation of resources and legislative and government attention to these issues.

The Future

22. In the closing session the participants were briefed on the recent initiatives of the Law Commission of England and Wales and of governments in Canada to assist in reform of the law and harmonization of the law dealing with those legal subjects discussed at the forum. The techniques for practical and orderly reform of the law in both countries were outlined. The importance of widespread consultation with industry, users, and the professions was stressed, as was the importance of avoiding excessive overreach of the law or the enactment of laws which unduly depart from basic legal principle or diminish due process. The possibility of designing a general law against "hacking" was explored. A "two track approach" to the aspects of fraud in international movements of financial information, was proposed, viz:

- The development of *domestic* law which deals with international aspects of fraud and authorizes the exercise of local jurisdiction over offenses having connection in any of their overt acts with the jurisdiction involved; and

- The development of *international* law with immediate emphasis on improvements in the law of extradition and mutual assistance.

The particular problems of fraud, faced by multinational banks and other financial institutions were reviewed. It was suggested that such bodies should work towards developing a code of cooperation to effectively tackle the identified interjurisdictional aspects of the problem. The framework of law for the legal protection of various aspects of information was also mentioned: criminal law, civil law obligations, trade secrets law, copyright law, the law of confidence, laws for the protection of privacy and for access to information (Freedom of Information Act). It was urged that the participants should follow up, in their home jurisdictions, the subject matters of the forum. It was also stressed that other major issues compete with these forum topics for the attention of national lawmakers and international agencies. The caution and slow moving process of lawmaking in democracies were emphasized. One practical way of encouraging government and the private sector to notice the issues was likely to be by calling attention to the loss of public and private revenue involved both now, and potentially in the future. The beginning of wisdom, it was suggested, was the meeting of minds across national borders; that was why the forum had been both timely and valuable.

Toronto Statement on Vulnerability of Financial Transactions

23. At the conclusion of their deliberations, the participants turned to a consideration of a Summary Record setting out their chief concerns and expressing their opinions on some of the most important initiatives that might arise out of the forum in Toronto. They accepted, by consensus, the Toronto Statement on the International Legal Vulnerability of Financial Information. That Statement is the frontispiece to this Summary Record.

Appreciation

24. The participants recorded their thanks to The Royal Bank of Canada for providing facilities for the forum, to the sponsoring organizations for their initiative in convening and supporting the meeting, to Dr. Peter Robinson and Mrs. Anne Branscomb for planning the meeting and to the chairman, rapporteurs, and paper writers.

Toronto, Wednesday, 28th February 1990

III. FURTHER DEVELOPMENTS

The Toronto Conference has provided the impetus for the creation of a new OECD expert group on security of information systems. The group had its first meeting in Paris on 4 and 5 January 1991, and its sec-

ond meeting on 4 and 5 March 1991. These actions indicate the sense of urgency felt by many sectors about the need for agreed international guidelines on data security issues.

Between 1978 and 1980, an earlier OECD expert group on transborder data barriers and the protection of privacy produced a set of guidelines which were eventually adopted by all twenty-four OECD member countries. The new group hopes to emulate this success by securing agreement on the basic principles to be observed in laws and policies on data security and thereby to produce a further set of guidelines.

The new expert group has before it draft guidelines prepared by the OECD secretariat dealing with such issues as:

- Assurance of the confidentiality of data;
- Assurance of the accessibility to data for those entitled to have such access; and
- Protection of the integrity of data, once assessed.

An interesting feature of the participation in the new expert group is that it is not limited to representatives of OECD member countries. Representatives of a number of multinational private sector organizations having an interest in data security are also taking part as observers. This innovation may mean that, once formulated and incorporated into national laws, the new principles may be more readily accepted as meeting the interests of a wider group of those whom they affect.

The Toronto conference provided an important stimulus to the establishment by the OECD of its new expert group. To that extent it may have contributed to an important exercise in developing international guidelines. Not all conferences produce such a useful and practical outcome so quickly.

Annexure A
Sponsoring Organizations

The views expressed in the attached Statement and Summary Record do not necessarily reflect the opinions of the sponsoring organizations which did not seek in any way to influence the free expression of views by the participants:

Bank of America

Barclays Bank

FISC (The Center for Financial Industry and Information Systems), Japan

The Hong Kong and Shanghai Banking Corporation

The Royal Bank of Canada

Westpac Banking Corporation

Participants

The organizations named identify the affiliation of participants who expressed personal views only. The opinions in the Statement and Summary Record should not be attributed to the organizations named.

Brian Bawden	Osler Hoskin & Harcourt
Thomas C. Baxter, Jr.	Federal Reserve Bank of New York
Leonard M. Bellam	The Royal Bank of Canada
J.J. BloomBecker	National Center for Computer Crime Data
Roland Brandel, Esq.	Morrison & Foerster
Anne W. Branscomb	The Raven Group
James Brundy, Esq.	Bank of America
Richard Buxton, Q.C.	Law Commission of England and Wales
Fred R. Cohen	The Chase Manhattan Bank
William Cook	Computer Fraud and Abuse Task Force
Bradley Crawford	McCarthy Tétrault, Barristers & Solicitors
Ian Cunliffe	Blake, Dawson, Waldron, Australia
Prof. Dr. B. de Schutter	Vrije Universiteit Brussel
N.A. Doucette	RCMP
Gaylen Duncan	CMHC
Eric Ellen	Director, ICC International Maritime Bureau
Saul Froomkin, Q.C.	Attorney General, Bermuda

James C. Grant	The Royal Bank of Canada
Irwin L. Gubman	Bank of America
Charles Holland, Jr.	Citicorp Technology Office
Prof. Masao Horibe	Hitotsubashi University
The Hon. Michael Kirby	Supreme Court of New South Wales, Australia
Susan Lautz Kirk	Bank of America; Chairman, International Computer and Technology Law Committee, International Bar Association
Sandra M. Lambert	Security Pacific Corporation
Edward G. Lee	Department of External Affairs, Canada
William List	KPMG Peat Marwick McLintock
J. Fraser Mann	Borden & Elliot
Patrick McDonough	AT & T
Det. Supt. Brian Newbury	West Midlands Police
Trevor Nicholas	Barclays Bank
Susan Nycum	Baker & McKenzie
Ernest Patrikis	Federal Reserve Bank of New York
Alice Pezard	Direction du Trésor, France
D. Piragoff	Department of Justice, Canada
D.C. Préfontaine, Q.C.	Department of Justice, Canada
Mark Rasch	Department of Justice, USA
Lucy H. Richards	Bureau of International Communications & Information Policy, USA
Dr. Peter Robinson	Atwater Institute, Canada
J.E. Strickland	Hong Kong & Shanghai Banking Corp.
Shigemi Tanaka	F.I.S.C.
Mark Tantam	Serious Fraud Office, England
Morinosuke Tsuchiya	F.I.S.C.
David A. Williams	Westpac Banking Corporation
W.M. Wilson	Bell Gully Buddle Weir
Prof. Kiyoshi Yasutomi	Keio University

Observer

Yoshiki Mine — Delegation of Japan to the OECD

Annexure B
"INTERNATIONAL LEGAL VULNERABILITY OF FINANCIAL INFORMATION"

Toronto, Canada

26-28 February, 1990

PROGRAM

SESSION 1: SUBSTANTIVE LAW — FEBRUARY 26: 9:00-12:00 NOON

Chair:

Anne Branscomb	Program on Information Resources Policy, Harvard University, Cambridge, MA, USA

Criminal Aspects

Mark Tantam	Serious Fraud Office, London, UK
Masao Horibe	Professor of Law, Hitotsubashi University, Tokyo, Japan

Civil Aspects

Susan Nycum	Baker and McKenzie, Palo Alto, CA, USA

Bankers' View on Problems

James Grant	Executive Vice President, Royal Bank of Canada, Toronto, Canada
Trevor Nicholas	Director Information Systems and Resources, Barclays Bank, PLC, London, UK
David Williams	Head of Strategic Operational Risk, Westpac Banking Corporation, Sydney, Australia
Irwin Gubman	Senior Vice President and Associate General Counsel, Bank of America, San Francisco, CA, USA
Tom Baxter	General Counsel, Federal Reserve Bank of New York, New York, NY, USA

SESSION 2: PROCEDURAL LAW — FEBRUARY 26: 14:00-17:00

Chair:

Patrick McDonough	Chair, Computer Crime Committee, American Bar Association, Chicago, IL, USA

Collection of Evidence

Eric Ellen	Director, International Maritime Bureau, International Chamber of Commerce, Barking, UK
Kiyoshi Yasutomi	Professor of Law, Keio University, Tokyo, Japan

Victimization & Police Cooperation

Norman Doucette	Assistant Commissioner, and Director, Economic Fraud Unit, Royal Canadian Mounted Police, Ottawa, Canada

Priority Issues

J.J. BloomBecker	Director, National Center for Computer Crime Data, Los Angeles, CA, USA
Brian Newbury	Officer in Charge, Fraud Squad, West Midlands Police, Birmingham, UK

SESSION 3: INTERNATIONAL COOPERATION:
JURISDICTION AND HARMONIZATION — FEBRUARY 27: 9:00-12:00 NOON

Chair:

Dr. Peter Robinson	Visiting Fellow, Atwater Institute, Canada

Public International Law

Edward G. Lee	Legal Advisor, and Assistant Deputy Minister, External Affairs, Ottawa, Canada

Jurisdictional Questions

Ian Cunliffe	Blake Dawson Waldron, Sydney, Australia

Harmonization of Substantive Law

Criminal Law

Alice Pezard	Ministére de l'Economie des Finances et du Budget, Direction du Trésor, Paris, France
Donald Piragoff	Senior Counsel, Department of Justice, Ottawa, Canada

Civil Law

Roland Brandel	Morrison & Foerster, San Francisco, CA, USA

Harmonization of Procedural Law

W.J. Cook	Assistant U.S. Attorney, U.S. Department of Justice, Chicago, IL, USA
W.M. Wilson	Bell Gully Buddle Weir, Wellington, New Zealand

SESSION 4: INTERNATIONAL COOPERATION:
PREVENTIVE LAW AND
ALTERNATIVE APPROACHES — FEBRUARY 27: 14:00-17:00

Chair:

Susan Kirk	Chair, International Computer and Technology Law Committee, International Bar Association, London, UK

International Organizations: Present and Future Work

Bart de Schutter	Director, International Criminal Law Centre, The Free University, Brussels, Belgium

Prevention: Codes of Conduct

Gaylen Duncan	Senior Vice President, Canada Mortgage and Housing Corporation, Ottawa, Canada

Public Awareness

Saul Froomkin	Attorney General, Hamilton, Bermuda

Other Banking Aspects

William List	Partner, KPMG Peat Marwick McLintock, London, UK

Where are we heading?

Hon. Michael Kirby	President, Court of Appeal, Supreme Court, Sydney, Australia

SESSION 5: WHERE DO WE GO FROM HERE? FEBRUARY 28: 9:00-12:00 NOON

Chair:

Hon. Michael Kirby	President, Court of Appeal, Supreme Court, Sydney, Australia

Future Trends

Richard Buxton	Commissioner, Law Commission of England and Wales, London, UK
Daniel Préfontaine	Assistant Deputy Minister, Department of Justice, Ottawa, Canada

CONCLUSION