291

AUSTRALIAN COMPUTER SOCIETY INCORPORATED

IFEPS TECHNICAL COMMITTEE 6 (DATA COMMUNICATIONS)

SYMPOSIUM ON DATA COMMUNICATIONS, TECHNOLOGY AND PRACTICE

SYDNEY HILTON, 17 NOVEMBER 1981, 2.15 P.M.

DATA COMMUNICATIONS TECHNOLOGY

NATIONAL AND INTERNATIONAL LAW

The Hon. Mr. Justice M. D. Kirby
Chairman of the Australian Law Reform Commission

November 1981

AUSTRALIAN COMPUTER SOCIETY INCORPORATED

IFEPS TECHNICAL COMMITTEE 6 (DATA COMMUNICATIONS)

SYMPOSIUM ON DATA COMMUNICATIONS, TECHNOLOGY AND PRACTICE

SYDNEY HILTON, 17 NOVEMBER 1981, 2.15 P.M.

DATA COMMUNICATIONS TECHNOLOGY

NATIONAL AND INTERNATIONAL LAW

The Hon. Mr. Justice M.D. Kirby
Chairman of the Australian Law Reform Commission

OF LAWYERS AND COMPUTERISTS

Before I became Chairman of the Australian Law Reform Commission, and indeed before the Commission received from Attorney-General Ellicott its mandate to inquire into new Federal laws for the protection of privacy in Australia, I had no more conception of the computer and of the potential of data communications than other laymen. Mind you, I had read A.P. Herbert's apocryphal account, written in 1958, of the case of Haddock v. The Generous Bank Limited and Computer 1578/32/W1.[1] Computerists who, by and large are an even more serious breed than lawyers, would do well to introduce themselves to the challenges of the legal mode of thinking, by reading this case of the Rein of Error. In it, a computer is alleged to have been guilty of defamation of the good Mr. Haddock because, during a voltage failure, it produced an error in his banking account. But to an action against the bank for defamation, that cunning lawyer Sir Mordant Wheel raised the ingenious legal defence:

> The bank is not responsible, because the bank is unable to control the Computer.[2]

According to A.P. Herbert, the computer conducted an exquisite dialogue with the learned judge. And I am ashamed to say that on every occasion the computer came out best.

I suppose I had occasionally thought, as a layman, of the possible impact of data communications upon individual privacy. Like most laymen, I merely reflected the view of mixed awe and contempt for computerists to be found in Felicia Lamport's poem 'Deprivacy':

> Although we feel unknown, ignored
> As unrecorded blanks,
> Take heart! Our vital selves are stored
> In giant data banks,
>
> Our childhoods and maturities,
> Efficiently compiled,
> Our stocks and insecurities
> All permanently filed,
>
> Our tastes and our proclivities,
> In gross and in particular,
> Our incomes, our activities
> Both extra- and curricular.
>
> And such will be our happy state
> Until the day we die
> When we'll be snatched up by the great
> Computer in the sky.[3]

Then things changed. The Australian Federal Government committed itself in the electorate to an inquiry into privacy laws. Subsequently a commitment to the introduction of such laws was given to the Parliament. The Law Reform Commission embarked upon its inquiry and this inevitably took me into an examination of the penetration of Australian society by computers linked by telecommunications. The social and legal consequences of this extraordinary technology had to be examined, first with respect to privacy and later, when the Commission received another reference, with respect to its implications for the presentation of evidence in Federal and Territory courts.[4] During these inquiries, my attention was diverted more than once to the many other implications of the new data communications technology for the law, for society and for the legal profession.

In 1978, when the Organisation for Economic Co-operation and Development (OECD) in Paris launched its endeavour to establish Guidelines on trans border data barriers and the protection of privacy, I was sent to the relevant Expert Group, as Australia's representative. I was elected Chairman of the Group and took part in the preparation of the Guidelines, which have since been adopted in the form of a Recommendation by the Council of the OECD.[5] As will be disclosed, Australia is now one of the few OECD countries which has not ratified the Guidelines. But they form part of international jurisprudence. Taking part in their development, as I did, I had the opportunity to see the way in which the technology of data communications is already stimulating the development of international law.

THE AGE OF 'COMPUTICATIONS'

I recount these personal details, not out of any sense of false pride (for all significant achievements in this area still lie ahead) but in order to explain how it is that a judge and a lawyer should wander across such otherwise unfamiliar territory as the world of informatics. A French Minister, in an unkind moment of retaliation against technological Franglais, coined the new word, informatics 'computications' to describe the phenomenon we are talking of.[6] Whether we adopt his word, 'informatics' or talk of 'data communications', there is no doubt that the technology in which the participants in this symposium are involved has enormous ramifications for society, including international society.

One lawyer who knows something about these things described the invention of the computer as 'the greatest contribution to the quality of human life since the development of language'.[7] He went on to describe some of the implications for the law. In the short space of time available to me, I must necessarily be superficial and selective. My thesis can be briefly stated. It is that such a dynamic technology, so rapidly penetrating the economies of all OECD countries and beyond, is bound to present novel social and legal problems at national, subnational and international levels. We run the risk that our institutions of lawmaking will not be able to cope with the implication of the new technology for legal change. The Law Reform Commission in Australia (and the work of expert committees in the OECD) can help us address the national and international problems that are presenting, and to do so with the facility of a proper community debate. However, the problems are as numerous as they are complex. They present, like the advances in the technology itself, with ever-increasing speed. They suggest that we should search out the normal solution for difficulties of this kind, adopted in English-speaking countries. I mean the establishment of routine institutions and procedures to consider efficiently and with appropriate expertise, the social, economic and moral implications of the rapid technological advances.

No-one doubts the speed with which data communications are penetrating national and international markets. Although available figures are not entirely satisfactory, one comprehensive review done over a three-year period by the Australian Bureau of Statistics for the Committee of Inquiry into Technological Change in Australia, found that more than three-quarters of large-type enterprises introduced a technological change of at least one type. The majority of large enterprises (60%) introduced ADP equipment for the first time, or ADP equipment of a type different from that used previously. The growth of this technology in Australia was described as 'rapid'.[8]

Linkage of computers by telecommunications has produced an exponential growth in the movement of information. This still continuing. It was reported to the OECD in 1980 that important new patterns are emerging in data communications. Approximately 13,000,000 data communication transactions take place each day in Western Europe. Of these, approximately 10% are international. This ratio contrasts with voice traffic, where only 1% of transactions are international. Data communications have already overtaken telex in terms of total flow of traffic. The total number of data communications transactions in Western Europe was expected to increase at a compound annual rate of 25% in the period 1979-1987. The number of international data communications transactions was estimated to increase at an annual compound rate exceeding 30%.[9] Similar developments can be expected in Australia. Indeed, we may go further because of the continental size of our country and our geographical isolation with traditional areas of cultural and economic concern.

The comprehensive implications of this growth in data communications have been explored by reports in many countries.[10] Obviously, the implications include the impact of the new technology on employment, on the greater vulnerability of the wired society to terrorism, accident and mistake[11], the implications for the telecommunications monopoly and for tariff policies governing the movement of information as well as the implications for international relations, national security and defence and relations with non-computerised developing countries.[12] These are not the subject of this paper. It surveys a different scene: the implications of the new technology for the law and for lawyers. Obviously, however, the wider implications must be watched. A society of diminishing numbers of privileged workers, with declining work of a routine character, may engender social tensions that require legal attention. A more vulnerable society may demand laws which require duplicate holdings of at least some vital national data, special security against terrorism and accident and, possibly, the licensing and policing of some computer systems, at least where society is specially dependent upon them.

The standardisation of technology to provide better back-up facilities where things go wrong, self-sufficiency within areas of computer operation to prevent widespread haemorrhage of problems and, possibly, the limitation of dependence on some foreign sources, at least where specially vital or sensitive areas are involved, may require legislative guidance for the computerists of the future.[13] For present purposes, it is enough to show that the technology is new, that its introduction is rapid and pervasive and that it brings in its train many problems which will not go away: including legal problems.

COMPUTERS AND PRIVACY

Data communications developments alone do not explain the contemporary challenge to individual privacy. Other considerations are relevant including the growth of the powers of entry, search and seizure afforded to ever-increasing numbers of government officials and new, intrusive business practices, such as direct marketing, door-to-door canvassing and the like. Related technologies are relevant, such as the technology of surveillance and the special power of the modern media unfairly to intrude, without justification, into the individual's private life.

But, overwhelmingly, the pressing international concern about the diminution of individual privacy is the result of the perceived potential of informatics to reduce the control and even the knowledge which the individual has of the way others are perceiving him. From a primitive interest to defend the individual's person, through the interest to protect the territory and property immediately surrounding him, the modern concern of the law to defend a zone of privacy, is addressed to the information penumbra concerning an individual, on the basis of which he may be perceived by others and relying upon which decisions may be made vitally affecting him.

The features of automated personal data systems which attract concern have been catalogued in numerous studies. The 1980 discussion paper of the Australian Law Reform Commission, Privacy and Personal Information, listed the following characteristics as those said to raise new dangers for individual privacy:

- Amount. Greatly increased capacity for storage of personal information.
- Speed. Significant improvements in the speed and ease of retrieval of information.
- Cost. Substantial reduction in the cost of handling and retrieving personal information.

New Profession. Creation of a new group of technicians and professionals not subject to traditional constraints applicable to the established professions.

- Linkages. The possibility of effective cross-linkage between different information systems.
- Profiles. The possibility of constructing composite 'images' of individuals.
- Accessibility. Reduction of the intelligibility of personal information and inhibition in access by individual subjects to that information.
- Centralisation. Readier centralisation of control over information and ease of access to it by those with relevant power or specialised skills.
- Trans Border Data Flows. Storage of personal information in overseas countries, with the exponential growth of trans border flows of data.

As a result of domestic recognition of these problems and of practical instances of perceived unfairness and oppression, actual and potential, in automated personal data systems, legislation has been enacted in a number of countries, directly or indirectly aimed at the protection, quality control and security of automated personal data.[14]

The growth of trans border data flows and the capacity of the new technology to circumvent or frustrate domestic laws on data protection and data security led to moves after 1971 to establish an international regime which would at the one time ensure safeguards for individual privacy and also limit undue interruptions to the free flow of data, including personal data, between nations.

In the Council of Europe a committee of experts was established in 1971 specifically to address the protection of privacy with respect to the use of computers. As a result of the report of that committee, two resolutions were adopted by the Committee of Ministers of the Council of Europe. The first, in September 1973, annexed certain principles relating to personal information stored in electronic data banks in the private sector. The second, adopted in September 1974, annexed like principles for the public sector. These resolutions have greatly influenced the initiation and design of European laws on data protection and data security.

In November 1973 the Commission of the European Communities delivered a report to the EEC Council proposing a Community policy on data processing. Although the focus of this report was the need to develop a viable European information technology industry, it concluded that the linkage of data banks, nationally and supra-nationally, would require the establishment of common measures throughout the Communities for the protection of its citizens. By 1977 a committee of experts of the Council of Europe had been instructed to prepare a draft International Convention for the Protection of Individuals 'with Regard to Automated Data Files'. It was contemplated that the Convention would be open to adherence by non European countries. The final draft of the Council of Europe Convention was approved by the committee of experts in May 1979 and adoption by the Council early in 1981.[15]

So far as Australia is concerned, the effort of the OECD to define a framework for laws governing data communications is of livelier concern. The OECD has been examining the social implications of data communications at least since 1969. The Expert Group to which I was appointed was the culmination of ten years of OECD activity. Its report was transmitted to the Council of the OECD which, in September 1980, by resolution adopted recommendations commending the proposed Guidelines to member countries, urging them to take them into account 'in their domestic legislation', to 'endeavour to remove or avoid creating unjustifiable obstacles in trans border flows of personal data' and to 'co-operate in the implementation of the Guidelines'. Several countries abstained from the recommendations, including Australia. The United Kingdom abstention was withdrawn on 23 September 1981 when that country endorsed the Guidelines. The position has now been reached that of the 24 member countries of the OECD, only Australia, Canada and Turkey have not subscribed to the Guidelines. The Turkish abstention relates to the military government. The Canadian abstention relates, apparently, to sensitivity to United States dominance of data communication. The United States was recently described as the 'OPEC of information'.[16] The Australian abstention was to permit consultation with the States. The Minister for Science and Technology, Mr. David Thomson, recently announced his hope that Australia would shortly be able to adhere to the Guidelines. Certainly, in the work of the Australian Law Reform Commission, we are attending most closely to the Guidelines in the development of our proposals on Federal privacy protection.[17]

The Law Reform Commission has concluded that present Australian law does not provide adequate protection for privacy, including in respect of personal information stored and transmitted in electronic form. The Commission has suggested that the general principles collected in the OECD Guidelines should be adapted for incorporation in Australian domestic law.

Under the leadership of Associate Professor Robert Hayes, the Commissioner in charge of the privacy reference, the Commission hopes to conclude its report on this wide-ranging topic early in 1982. Clearly, there is an element of urgency. Numerous articles in the professional and popular press have called attention to the dangers of a 'world data war'. A recent item in the New Scientist pointed out that:

> the lack of uniformity among developed countries in data regulation may lead to problems when an organisation in one country wishes to transfer computer data to another country. ... unless the data rules in the two countries compatible, the transfer may not be permitted. Firms in Britain could be at a particular disadvantage as, despite years of discussions, the UK has no regulations regarding data flow and so is severely out of step with other countries in the industrialised world.[18]

Already cases have arisen where the export of personal data from a country with data protection laws has been forbidden to a country unable to offer equal protection against the haemorrhage of sensitive personal data. The classic example is that of the Siemens company in Sweden which wanted to transfer personnel files from its Swedish branch to its headquarters in Munich. Permission was refused. Another well known example where permission was refused involved the Health Department of a Swedish county authority which was prevented from ordering, from a British firm, 80,000 plastic cards which contained personal information in computer code about Swedish citizens. The risk that 'shadow' registers on Swedish people could be established in other countries, outside the reach of national law, was deemed too high. A new phenomenon appears on the scene in the development in Third World countries of limitations on trans border data links where data processing alternatives exist within the country or where external interests control access to the foreign data banks. There is a legitimate concern about the risks of data protectionism and about data fiscal policies. I will put the latter no higher than to say that, despite a traditional reluctance to tax information and information flows, anything growing at such an exponential-rate and measurable-rate as data communications must inevitably attract the ever-hungry eye of the inventive tax gatherer.

COMPUTERS AND EVIDENCE

The development of the computer poses many other problems for domestic law. Amongst these none is so urgent of resolution and frequent in manifestation as the need to modify the law of evidence to permit more readily the admissibility in court trials of computer output. The basic problem is the hearsay rule which forbids the admission at a trial of evidence, oral or documentary, which cannot be deposed to, from his own knowledge, by the person giving evidence before the court. This rule is itself an outgrowth of the continuous oral adversary trial of the common law. It has been influenced in its development, and in the exceptions which have grown up, by the system of jury trial. But it is also grounded in principles of fairness: that litigants should be able to face and test by cross-examination their accusers, that courts should base their decisions only on reliable and, where necessary, tested and scrutinised information, and that in the solemn business of judicial determination, particularly where liberty is at stake, the means should be available to check and verify material before the court. The advent of photocopying, data processing and electronic communication and their widespread use throughout the community, render the maintenance of these rules in their present state unreasonable and indeed impossible. It would be intolerable to require that every person who has contributed to a computer record should be available to prove his or her contribution to a computer record. That was difficult enough and already unreasonable in the case of business records before computerisation. It becomes even more unreasonable when computerisation is adopted. Unhappily, for the solution of this problem, there remains the abiding difficulty that mistakes do occur. It is simply not appropriate to accept, without any precaution or reservation, the printout of any computer as if the technology were a guarantee of accuracy and, in some magical way, provided protection against false, negligent or even maliciously misleading information.

Attempts have been made, by legislation, to provide for the admission of computer-generated evidence. In the United States, the most common form of such legislation is an elaboration of an exception to the hearsay rule adopted earlier to cope with business records of large and impersonal corporations. The adoption of this exception made it easier for State and Federal efforts at uniform law reform to provide a regime for computerised material, most of it being business records. In England, an amendment to the Civil Evidence Act in 1968 provides for the admission, under given circumstances, of a 'statement contained in a document produced by a computer'.[19] In Australia, a number of law reform reports and a series of statutory provisions[20] have sought to provide for admission, under specified conditions, of data communications and computer-generated data.

The Australian Law Reform Commission is now seeking out a more fundamental principle by which probative evidence of this kind can be admitted in evidence in courts of law. A major aim of the inquiry must be the reduction of the disparity between the community's use of information and the availability of that information for authoritative decision-making when a dispute arises. The existence of unacceptable differences between the material accepted as reliable and relevant in everyday life, on the one hand, and the evidence admitted when an issue has to be resolved in court, on the other, should not be allowed to persist. Otherwise, the courts will be regarded as unnecessarily obstructive, resistant to changing realities and unrealistic and unhelpful in their approach to resolving issues in dispute.

COMPUTERS AND CRIME

Towards the end of 1980 officers of the Australian Federal Police were reported as urging yet another task for the Law Reform Commission, relevant to the 'informatisation' of Australian society. Within the administration, and now publicly, the need for a national and comprehensive inquiry into the implications of computerisation for the criminal law has been discussed.

Some antisocial conduct involving computers will fall within the terms of current criminal offences. In Europe and North America concern about the perceived dangers to employment and liberty have already led to attacks upon computer centres and the destruction of computer equipment. Such conduct may be liable to be prosecuted under current crimes relating to malicious damage to property, arson and the like. The problem of computer crime in this context is likely to be less the adaptation of the language of present criminal offences than the inadequacy of current maximum penalties. As has already been stated, the capacity of the computer to centralise vital and often unduplicated data can result in unprecedented dislocation, when the data base is destroyed or significantly interrupted.

It is when one turns to the fraudulent misuse or manipulation of computerised data, that even greater problems arise. Here, not only must the difficulties of proof be addressed. Even if the law of evidence is amended and if penalties are increased to reflect the huge financial losses to the victims that may be involved, other problems remain. One of these, rather intangible in character, is the difficulty which police have in tracking down and prosecuting cases of computer fraud, extortion and manipulation. The victims of such crimes are very often large, impersonal corporations, sometimes even capable of absorbing substantial losses. Society often finds it difficult to understand, and then to appreciate the antisocial quality of, computer fraud.

Moreover, police are not always equipped, by training to have a sufficiently thorough understanding of computer technology, successfully to track down and prosecute offenders. Sometimes, the amount at stake is so great that corporations may be tempted not to involve the police. Often the personnel involved have been hitherto trusted members of staff. The embarrassment of detection and the disclosure of weak internal procedures may provide a motive for 'internal' resolution of the problem. Furthermore, more than one commentator has pointed to an additional problem, namely that computer criminals are typically young, highly intelligent and often likeable characters with no difficulty of rationalising and defending their actions.

An addition problem, bound up with the need for reform of the law of evidence, is the difficulty of prosecuting complex computer frauds before a lay jury. The South Australian Commissioner for Corporate Affairs explained this difficulty thus:

> If the computer remains an unknown, 'orwellian' device to all but a few trained experts, how can we expect a lay jury to properly comprehend the way in which a computer was used to effect a fraud possibly running into millions of dollars? ... Courts, juries and witnesses spend a vast amount of time engaged in the hearing of [matters of 'formal proof'].[21]

Solutions to this procedural difficulty include simplification and reform of the law of evidence, procedural changes to require pre-trial conferences to settle the 'real' issues for trial and provision, either compulsory or on election, for trial by judge sitting alone.

Transcending all of these difficulties is the problem of characterising antisocial activities involving computers by reference to currently existing and appropriate criminal offences. Theft is traditionally defined as carrying away the property belonging to another with the intention of permanently depriving the owner of the possession of it. But in the case of a computer, the true loss may occur without any asportation of the computer hardware or even the software. Access at a terminal to vital information may suffice. Copying or transferring that information may involve no carrying way of identifiable property. Though in England, following the Theft Act 1968, the English Law Commission has concluded that the misuse of a computer to steal money from a bank or property from an owner would be punishable within the present definition of 'theft', the same may not be true in those Australian jurisdictions which have not followed the Theft Act. The problem is not an academic one. In Ward v. The Superior Court of California[22] an employee of a computer firm secured the transmission of programs of a rival firm into his own computer's stored memory.

He ...ien made a copy of the programs. Charges were laid under the Californian Penal Code relating to provisions governing theft and trade secrets. In that code 'articles' for the purpose of theft is very broadly defined. Nevertheless, it was held that the electronic representation of the program contained in the computer memory could not be regarded as an 'article' within the scope of the definition. The criminal law is traditionally interpreted with strictness. Offences designed before the advent of informatics may not, in terms, apply to conduct which, admittedly 'wrong' and harmful in a moral sense, is nevertheless not caught up by current penal characterisations.

It is important to stress the utility of stigmatising certain acts involving the misuse of computers, as criminal. To do so 'fortifies the social pressures against [their] commission and has a salutory effect upon business practice'.[23] Numerous offences have been created in the United States to deal with computer crimes.[24] In Australia, the Standing Committee of Attorneys-General is already examining some of the issues relating to computer crime, particularly in relation to investigation and prosecution of such crimes. The need for a thorough and open national examination of the relevant substantive law seems overdue.

OTHER INTERNATIONAL ISSUES

Every new technology with international implications ultimately produces an international legal response. The development of radio produced the ITU Charter in 1876. Civil aviation produced the Warsaw Convention in 1929 and subsequently the Hague Protocol and the Guadalajara Convention referred to in the Australian Civil Aviation (Carriers' Liability) Act 1959. The exploration of space resulted in the Outer Space Treaty in 1967. In a like manner, the developments of international data flows will plainly require development of new international principles. It would be preferable that these principles and any international conventions or other legal rules should be developed only after careful study. One of the problems facing the international community (as it faces countries in domestic jurisdiction) is the speed with which these developments occur.

It is difficult to sort out legal implications of trans border data flows and to distinguish them from economic concerns. Few issues are of a purely legal nature in an area such as this. However, a checklist of matters that will rapidly require international treatment would certainly include:

. Provision for conflict of laws i.e. determination of the law that should govern data transactions in a technology that is virtually instantaneous and sometimes involves the constant movement of data, so that it is not (as previous media were) in a fixed, identifiable or discoverable place. The laws of which country apply to data that is constantly moved around, for reasons of economy, between data bases in different parts of the world?

. Extraterritorial application : normally domestic law, particularly criminal law, is confined to a given jurisdiction. But where there is or might be a link with a given country, this will frequently attract the application of local legislation. In dealing with an international medium, to what extent is it realistic to seek to impose domestic regulation? The risk of a cacophony of domestic laws impacting the worldwide movement of data is either that the law will be ignored or that it will create tremendous confusion and diseconomy.

. Copyright : recent amendments to the Copyright Act, now being absorbed in Australia, are quite possibly already overtaken by new data communications technology. The problem of applying copyright law, which developed in an era when it was adequate to protect the medium, may not be appropriate when we move to an era where the 'medium' and the 'message' may be divorced or the medium may be ephemeral in the extreme whilst the valuable information stands unprotected.

. Electronic fund transfers : the worldwide development of EFT raises many implications of policy but also a number of legal concerns. So far as I am aware these are not being considered, on an official level, in Australia, and calls have been made for the legal, social and economic implications of EFT to be studied as a matter of urgency.

International bodies already exist to consider some of these issues. For example, the World Intellectual Property Organisation may be the appropriate body to scrutinise the development of copyright law. The issue of conflicts of laws might be appropriate for consideration in the Hague Conference on Private International Law. That conference has specialised over many years in the study of conflict of laws questions. The OECD has been suggested as an appropriate forum for considering many of these international data and law questions.

It has been suggested that the development of disharmonious and restrictive domestic laws in the 19th and 20th centuries impeded the development of the world economic order and produced very serious conflicts of laws problems, many of which we have still not worked out. One author put it thus:

> Since ancient times and until the emergence of modern national states, the law governing maritime commerce had been large uniform in the western world. In the 18th and 19th centuries, legislative enactments and judicial practices in pursuit of narrowly conceived national interests gradually displaced in various countries the venerable and uniform 'law of the sea' and gave rise to sharp conflicts of laws. The movement of goods from country to country was thus hampered at a time when advancing technology and the spreading industrial revolution were about to lead to an expansion of maritime commerce on a world scale.[25]

The United States Delegate to the OECD in June 1980 urged that the collective task of members of that Organisation should be to foresee and help avoid like difficulties in the international flow of data. But unless positive efforts are put in train, the likelihood must be faced that differences in domestic law will arise and many questions, requiring international resolution, will be left unanswered. Amongst the latter are questions of procedures and remedies, including institutions for the adjudication of disputes involving international data communications:

> Should cases arising in the future be adjudicated in the first instance by national courts, an international judicial forum, the International Court of Arbitration, a new limited jurisdiction body, or in some other way? If it is the consensus that new principles of law must be developed, a further question is presented whether an international solution is best approached through a treaty, development of a Uniform Law, International Guidelines, or some other device.[26]

It is to be hoped that we take a warning from what happened in the case of the international movement of goods in previous centuries. Perhaps the very technology of data communications itself will facilitate and expedite the rapid meeting of minds, in different parts of the world, that is the prerequisite to the development of an appropriate international legal regime.

CONCLUSIONS

This paper has done no more than to identify some of the national and international problems that arise for the law as a result of the exponential growth in data communications within and between countries. In Australia, the Law Reform Commission is assisting the lawmakers to face up to some of the consequences of the new technology in the area of privacy protection and evidence law. Other concerns remain, some of which I have identified.

In the international field, the OECD Council has already adopted Guidelines on trans border data flows and the protection of privacy. Although Australia is one of the few remaining members not yet to have subscribed to these Guidelines, they are certainly in the forefront of the collective mind of the Law Reform Commission. If we can get compatability in domestic data protection and data security laws, that will, in itself, contribute to a reduction in the impediments that might otherwise arise in beneficial transborder data flows.

Other tasks of international law remain to be tackled. Some of these have been listed and the OECD may once again provide a forum, specially useful to Australia, for development of appropriate legal principles. Certainly, the subjects of conflicts of laws, the extraterritorial application of laws, the laws governing intellectual property, information rights, carriers' obligations, electronic fund transfers and procedural remedies, all deserve close and urgent attention.

The story of the interface of law and data communications is not a wholly depressing one. Lawmakers and law reformers are already using computer technology to assist them in their daily tasks. The statute book and case law are already partly 'on line' in Australia. Information technology will undoubtedly assist in many fields of lawyers' work. The effective implementation of freedom of information laws and of access to data will undoubtedly be facilitated by the growing automation of that data. At the same time, both for advocate and attorney, much routine work will be taken over by the computer. The challenge before the legal profession in Australia and elsewhere today is overwhelmingly one of relevance: finding new tasks appropriate to the history and training of the lawyer. It is to be hoped that there will be an adequate dialogue between lawyer and computerist. Out of such a dialogue should grow a greater appreciation by technologists of the values in society which the law seeks to uphold. But there is also needed an appreciation by lawyers of the implications for their discipline and work of the remarkable technology of data communications.

Perhaps lawyers may in the process even catch something of the infectious, dynamic spirit of inventiveness that so profoundly marks the contemporary technology of information.

FOONOTES

1. A.P. Herbert, Wigs at Work, 1966, 201.

2. ibid, 206.

3. Reprinted from Look.

4. Australian Law Reform Commission, Discussion Paper 16, Reform of Evidence Law, 1980.

5. Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Trans Border Flows of Personal Data, Paris, 1980.

6. N. Segar, French Minister for Telecommunications, Opening Address, Conference on Information Technology and Society, Paris, 24 September 1979.

7. C. Tapper, Computers and the Law, London 1973, xv.

8. Committee of Inquiry into Technological Change in Australia, Technological Change in Australia, Canberra, 1980, Vol. I, 59 (para. 3.184).

9. Statement made on behalf of Logica Limited, United Kingdom, to an ad hoc meeting on trans border data flows and data communication policies, OECD, document ref. DSTI/ICCP/80.27, 1.

10. Notably the report S. Nora and A. Minc, L'Informatisation de la Societe (Report on the Computerisation of Society), Paris, 1978 (France) and report of the Consultative Committee on the Implications of Telecommunications for Canadian Society (Clyne Report), Ottawa, 1979 (Canada). There are many other notable reports, particularly in Scandinavia. See generally Privacy Protection Study Commission, Personal Privacy in an Information Society, Washington, 1977 (United States) and Report of the Committee on Data Protection, (Sir Norman Lindop, Chairman), Cmnd. 7341, London, 1978 (United Kingdom).

11. Report by a Swedish Government Committee (SARK), The Vulnerability of the Computerised Society: Considerations and Proposals, 1979 (Official English translation by John Hogg), Stockholm, 1979.

12. These and other issues were considered at a recent high level conference on Information, Computer and Communications Policies for the 1980s, sponsored by the OECD and held in Paris, 6-8 October 1980. See Transnational Data Report, Vol. 3, No. 8, December 1980, 1.

13. Swedish report, n.11.

14. Privacy laws relating to personal information have been enacted in Austria, Canada, Denmark, France, the Federal Republic of Germany, Luxembourg, Norway, Sweden and the United States of America. Such laws are under active consideration in many other countries.

15. Transnational Data Report, Vol. 3, No. 6 (October 1980), 1.

16. See F. Kuitenbrouwer, 'The World Data War', New Scientist, 3 September 1981, 604.

17. D. Thomson, 'Information Technology Week', (1981) 6 Commonwealth Record, 1013.

18. Kuitenbrouwer, n.16 above. See also Business Week, 14 April 1980 ('When Privacy Laws Hurt Trade'); The Economist, 25 October 1980 ('We Don't Worry, We're British'); New Law Journal, 18 December 1980, 1191 ('Privacy and the Press'); New Society, 26 March 1981, 547 ('Privacy Pariah'); Computer Bulletin, June 1981, 1. See also the statement made by Mr. Timoth Raison at the Council of Europe Ministers of Justice Meeting, Montreux, September 1981.

19. For discussion, see Tapper, Computer Law, 168.

20. Evidence Act 1905 (Cwlth), Pt. IIIA; Evidence Act 1898 (NSW), ss.14A-14C, 14CD-CV, 43C; Evidence Act 1958 (Vic.), ss.55-56; Evidence Act 1977-1979 (Qld), ss.92-103; Evidence Act 1929-1979 (SA), ss.59a-59c, 45-45b, 34c-34d; Evidence Act 1906-1979 (WA), ss.79B-79E; Evidence Act 1919 (Tas.), ss.40A, 81A-81Q; Evidence Act 1980 (NT), ss.42B; Evidence Ordinance 1971 (ACT), ss.28-45.

21. J.R. Sulan, 'Legal Aspects of Computer Crime: Is the Law Adequate?', Paper delivered to the Jubilee ANZAAS Conference, Adelaide, 1980, reprinted in Australian Crime Prevention Council, Forum, Vol. 3, No. 4 (1980), 37, 44.

22. 3 CLSR 206 (Cal) 1972.

23. Tapper, Computer Law, 99.

24. A. Bequai, Computer Crime, 1978.

25. A.N. Yiannopoulos, 'The Unification of Private Maritime Law by International Conventions', 30 Law & Contemporary Problems 370 (1965).

26. Statement by United States Delegation, OECD, 'The Legal Issues in Transborder Data Flow', June 1980, mimeo.