MITCHELL COLLEGE OF ADVANCED EDUCATION

BATHURST, NEW SOUTH WALES

SIXTH AUSTRALASIAN CORPORATE CRIME INVESTIGATION COURSE

14 JANUARY 1983

COMPUTER CRIME AND LAW REFORM

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

January 1983

MITCHELL COLLEGE OF ADVANCED EDUCATION

BATHURST, NEW SOUTH WALES

SIXTH AUSTRALASIAN CORPORATE CRIME INVESTIGATION COURSE

14 JANUARY 1983

COMPUTER CRIME AND LAW REFORM

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

PUTTING IT IN CONTEXT

On the 9th November 1982, the Acting Federal Attorney-General provided an answer to a question directed to ascertain whether he would make a reference to the Law Reform Commission concerning the increasing problems of maintaining the privacy of computer based data and meeting the growth of computer crime.[1] The Attorney responded that he was aware of the 'enormity and complexity of computer crime as demonstrated by litigation in the U.S.A. involving equity financial corporations'. He pointed out that the Australian Law Reform Commission already had a reference on the subject of privacy and was expected to report on that subject in 1983. He then added:

> I am considering the giving of a reference to the Australian Law Reform Commission on crime committed through, or in connection with, the use of computers and my Department has asked the Australian Federal Police to report on difficulties encountered in this connection. I expect to announce a decision on such a reference shortly.

The Australian Law Reform Commission is a small body with four full-time Commissioners and a total professional staff of nine officers. It is engaged in many major projects of significance for national law reform. Within recent weeks it has received three new, major projects dealing with admiralty law, foreign State immunity and service and execution of process. It is a sad reflection on our legal system that, as a country, we are prepared to spend so relatively little on its systematic improvement. The Law Reform Commission has plenty to do. The purpose of this paper is to illustrate the scope and urgency of the problem of computer crime in Australia. Some work is already being done on it by the Australian Federal Police and by a working party of the National Companies and Securities Commission. Whether this problem is tackled by the Australian Law Reform Commission or by some other body is less important than that it be tackled, urgently and thoroughly and with full expert and public participation..

Let me start my review by indicating how the Law Reform Commission has already become involved in certain aspects of the problem of computer crime. As the Acting Attorney-General pointed out, the Commission has for some years had a major project on the protection of privacy in Federal areas of concern. This project is led by my colleague Associate Professor Robert Hayes. It is now in its final stage. We are considering a draft report and draft legislation. Amongst subjects that will be tackled in the report are the factors that have led or are leading to an erosion of personal privacy in Australia. These factors include:

* the growing power of a wide range of officials, in addition to police, to enter property, search and seize persons and goods and otherwise invade territorial privacy;
* the growing brigade of private police and commercial practises which involve invasions of territory privacy by persons who are not officials;
* the increasing powers of surveillance, by highly sophisticated listening devices, telephonic interception and optical devices; and
* the dangers to the privacy of personal information flowing from the rapid penetration of computers in our society. The capacity of the computer to assemble and retain indefinitely greater masses of information, retrievable at ever-diminishing costs and ever-increasing speed and the capacity to match data and build profiles, all present the new problems of data security and data protection that require new laws.

In the course of my work on privacy protection, I was sent in 1978 to represent Australia at the meetings of an inter-government committee of experts convened by the Organisation for Economic Co-operation and Development (OECD) in Paris. This international agency brings together the technologically and economically advanced countries of Western Europe, North America and the Pacific region. I was elected chairman of the Committee. The issue before it was to devise Guidelines, the first step

towards international law. The Guidelines addressed the balance that should be struck in the rapidly growing international data traffic between laws governing the legitimate protection of privacy and the principle of the general free flow of information, seen to be economically, politically and socially beneficial. The Committee produced Guidelines which, in 1980 were adopted in the form of a recommendation by the Council of the OECD to Member countries.[2] Only two of the 24 OECD countries have not subscribed to the Guidelines. Australia is one of them. Our delay is said to stem from discussions between Federal and State officials. The great and powerful federations of the United States and Germany, the historic federation of Switzerland and countries as diverse as New Zealand, Japan and Finland could subscribe. As we all know, in Australia it is difficult to get agreement between Federal and State officials about anything - even the time of day.

In the course of my work with the OECD, I became aware not only of the tremendous growth of trans border data flows but of the many social and legal problems which these flows are creating and which lie unattended by lawyers and law makers. In September last year, I was invited to address the first session of a new committee of the OECD (the Committee for Information, Computer and Communications Policy) on legal aspects of the new information technology. I sought to chart a program for attention by the OECD to the common problems that are presented to our form of society by the new technology. Technological advances are happening so quickly. Problems of great complexity are being presented at such a pace. International co-operation provides the only effective way by which the democratic process of Western countries, including in Australia, can be helped even partly to keep pace with the social and legal fall-out presented by the new technology. As well, the international character of the technology, emphasised by the linkage of computers and telecommunications ('computications') made it apt that we should look at the problems, as we did in the privacy area, on an international level.

In the paper I delivered last September, the leaves of autumn falling on the Paris streets outside, I identified the following catalogue of problems for attention:

* further work on privacy protection;
* seeking compatibility in freedom of information laws;
* attention to vulnerability issues presented by the wired society;
* the legal implications of prolonged, structural unemployment;
* revision of private international law governing the determination of the legal regime to apply to legal dealings having an international component;
* the subject of informational sovereignty and informational protectionism;

* the revision of intellectual property law because of the fleeting ephemeral nature of computerised originality;
* the need for revisions of business law, the provision of liability for loss and error and the design of insurance against computer loss;
* the implications of the computer for evidence law and for the legal profession;
* computer crime and fraud.

In the multitude of legal problems presented in this long catalogue, I have to say to you that no concerted Australian effort is being made to tackled them. The Law Reform Commission will report in 1983 on aspects of the privacy implications of the new technology. It is also examining reform of the law of evidence in Federal courts, reform in part needed by the challenge of computer technology for our traditions of oral trial.[3] The Administrative Review Council is looking at some aspects of the implications of freedom of information laws. Perhaps the Federal Police are looking at some of the problems of computer crime. The proposed National Crimes Commission[4], when established, may develop a role in respect of sophisticated and computer crime law reform. But there is no body in our country bringing together study of the social and legal implication of the new technology. This is serious because the legal implications alone are many. The consequences of inaction and inattention or even slow and desolutary treatment will be damage to our society in generations to come.

I have now outlined the context of my interest in computer crime. It is both actual and potential. It is actual because of our current work in the Law Reform Commission on privacy and reform of the law of evidence. It is potential because the Federal Attorney-General is considering giving to the Law Reform Commission a general project on review of Australia's law to cope with computer crime. Clearly if such a review were to come, it would be necessary for the Commission to work closely with the Australian Federal Police and with the State police forces. The legal system and the policing system of Australia must renew themselves to meet the challenge of informatics.

COMPUTER CRIME: SUBSTANTIVE LAW

The first necessity of effective control of and sanction against wrongful and damaging conduct in respect of computers, is to provide laws which are adequate to characterise that conduct as unlawful, when it occurs. The range of anti-social activity which can involve computers includes:

* financial theft;
* property theft;
* computer software, program, information or data theft;
* unlawful access to computers;
* illegal use of computers;
* false accounting;
* furnishing false reports;
* malicious damage;
* ransom or hostage situations.[5]

Many of the wrongful and damaging acts which are done to or in relation to computing facilities are adequately covered by existing criminal law. For example, had he survived, the recent unhappy New Zealand man who endeavoured to blow up the Wanganui police computer in New Zealand, could have been charged with explosive offences, extortion, malicious damage and so on.

But, as has been disclosed in a number of cases in the United States, it is not always easy to squeeze clearly wrongful conduct in relation to a computer into bottles designed to contain earlier problems. The issue is one of legal 'characterisation'. For example, United States decisions held that theft of a program contained in a computer's memory could not, in some jurisdictions, be regarded as theft of an 'article' within the scope of the definition of the crime. The computer program was just not considered an 'article' within the context of the use of that word in the criminal statute.[6] Offences designed before the advent of computers may not, in terms, apply to the conduct complained of.

The common law definition of 'theft' itself involves carrying away the goods of another with intent to deprive that other of the permanent possession of the goods. But if the computer criminal simply gains access to data (possibly quite lawfully) he does not have to carry away 'goods'. He does not have to take the software program, let alone the hardware of the computer equipment. It may be sufficient for him to gain access to the data. In the United States, the implications of the linkage of computers to telecommunications in the context of computer crime was considered in the United States v. Seidlitz.[7] Seidlitz was charged with violating the Federal interstate transportation of stolen property statute. However, he was acquitted because it was held that the only thing that had crossed State lines was a series of impulses over telephone wires. It was suggested that such a transient impulse was not within the contemplation of 'interstate transportation' or 'property' when the statute was passed. There are also reports of a recent case in Canada. An individual was accused and convicted of illegal

use of telecommunication facilities when he had used a terminal to obtain unauthorised access to the university computer. On appeal to the Supreme Court of Canada, the conviction was quashed. One of the Supreme Court Justices said, in his judgment that if Parliament had felt that an unauthorised access to a computer should be punished, it would have passed an appropriate and specific law. If the mere act of copying data became a crime, he asked, where this would lead us in regard to the millions of photocopying machines now spread around the world.[8] The Canadian Government has apparently come to the conclusion, in the light of this decision, that the Criminal Code needs revision and it is taking steps to do this.

In some Australian States a broader definition of 'theft' has been adopted than existed at common law. The English Theft Act, adopted in substance in Victoria but not in other States, might, by offering a wider definition of 'theft' catch the manipulation of a computer to steal money from a bank or property from an owner.[9] The position of those States which have not adopted a wider definition of 'theft' and which adhere to the old definition at common law, with its emphasis on the carrying away of goods, may find, if challenged, that the law is not adequate to offer a basis for prosecution for the whole range of clearly wrongful acts performed by the manipulation of computers. The essential problem is that the computer has released the valuable commodity (information) from captivity in a permanent physical object (books and records). Punishable conduct of the past (breaking doors and windows, opening filing cabinets, taking files and valuable documents) all fell within the ambit of defined crimes. Furthermore, such conduct left a trail of useful in the detection and discovery of the criminals. The intelligent computer criminal of the future may never leave his terminal. In many cases, he may effectively destroy his trail because of inadequate security and audit arrangement in the computer program.

Even in Victoria, additional legislation has been proposed by Detective Chief Inspector K.E. Brown in a useful paper.[10] It is a proposal for amendment of the law of the State of Victoria. But, of course, the problem is a national one. Indeed, as Mr. Brown points out, it is an international one requiring urgent transborder attention.

The capacity of information technology to cross State and national boundaries presents a special problem for the substantive criminal law. There is a general principle, recognised in our courts, that crime is local, in the sense that domestic courts are normally confined to punishing criminal offences which occur in their own territorial boundaries or which have some other relevant territorial connection with the jurisdiction. You will recall the series of recent Australian cases which turned on the exquisite analysis of where a murder occured on the banks of the River Murray. Was it is Victoria and susceptible to Victorian law? Or was it is New South Wales and only punishable in the courts of that State?

This rule of international law is alive and well. It has been applied in many recent cases.[11] In the Stonehouse case, for example, the English House of Lords had to deal with an attempt outside the United Kingdom jurisdiction to commit a crime within the United Kingdom. Was this within the power of the English courts? In mid-1974, Mr. John Stonehouse had his wife take out five insurance policies on his life. He procured two false passports. On a trip to Miami he staged a disappearance whilst swimming. As he intended, the news was quickly transmitted to England by the media. His wife, ignorant of the deception, had made no claims on the policies when Stonehouse was discovered in Australia. The issue was whether the English courts had jurisdiction over the offence of attempting to obtain property by deception contrary to the Theft Act. The defence included that 'the final act alleged to constitute the offence of attempt had occurred outside the jurisdiction'. The House of Lords dismissed the appeal saying that the law 'must keep in step with technical advances in international communication'.[12]

But it is clear from this and other cases that where crimes are constituted of a number of elements, some of which may take place outside domestic jurisdiction by reason of access to international data communications, reform may be needed to ensure that the legitimate jurisdiction of local courts is not improperly frustrated by technical arguments based on confining the criminal law to entire acts all of them happening in a particular jurisdiction. That principle was all very well and good for the advent of computers linked by telecommunications. Nowadays, as has been illustrated by many cases, computer crime can involve elements occuring in a number of jurisdictions.

The Rifkin case is one of the most notorious. In October 1978, Rifkin a 32 year-old computer expert telephoned from a public phone box the communications room of a bank in Los Angeles and transferred $10.2 million from a non-existent bank account in New York City to an account with a diamond marketing company in Zurich, Switzerland. Rifkin flew to Switzerland to collect diamonds. He confided his activities to a lawyer friend. Unfortunately for him, the lawyer informed the FBI. It took the FBI agent 8 days to convince the bank of the theft. Rifkin was arrested and convicted of two counts of computer fraud.[13] Detective Chief Inspector Brown's comments:

> The ease with which the theft was committed, the complexities of tracing the transfer of money across State and international borders, the speed of its accomplishment and the lack of source documents identifiable with the perpetrator due to his ability to activate the transfer by telephone, indicates the problem facing law enforcement agencies in bringing this new breed of criminal to justice. Furthermore, it highlights the need for a greater international co-operation between police forces.[14]

COMPUTER CRIME: DETECTION

These are many cases like the Rifkin case. All too often, cases of computer crime are not discovered at all. All too often when they are discovered, they are discovered by accident. All too often, even when discovered by accident, they are not notified to the police. When notified, all too often there are difficulties of proof, difficulties of fitting the offence into current definitions into criminal conduct and difficulties of securing adequate punishment for the attractive, intelligent, bright-eyed person who is the typical computer criminal.

Take these cases:

* J. Polak was a purchasing agent in the County authority of San Diego U.S.A. He knew the troubles the County was having installing a new computerised system to control payments for goods bought. He set out to compromise the system. He created fictitious vendors, charging the County for non-existent supplies that had ostensibly been delivered. He collected approximately $50,000 in payments. He knew the system too well. Only his impatient questioning about a $70,000 cheque he was waiting for led to his detection.[15]

* The head teller at a bank in New York City was found to have stolen $1.5 million from the bank, but only when his bookmaker was raided and the records disclosed that he was betting up to $30,000 a day. In Denver, one Raymond Ressin financed numerous gambling trips to Las Vegas by falsifying the input to the computer of the stock brokers for whom he worked. He fraud too was discovered by chance.[16]

* There is the well known case of the criminal who had a sophisticated 'round-down' system. If there was a fraction of a cent in a bank account it was usually to be distributed over all accounts. Instead, this criminal set up a system where all such fractions were credited to his account. He named the account Zwana. It grew rapidly. His was the last in a series of customer accounts. It was only when the company public relations section tried to find Mr. Zwana to offer him an award that this criminal was ultimately caught.[17]

* J.N. Schneider developed a system to swindle Pacific Telephone Company. He found he could get the company to deliver parts to him for nothing because he had 'cracked' their computer system. Over 5 years, he stole approximately $250,000. When he was finally detected, it was not through any security procedures by the

telephone company or through investigation by law enforcement agencies. It was because one of his employees thought that he was not getting enough pay and this led to enquiries being made.[18]

* One case tells of a fraudulent transfer of $2 million. The culprit convinced his girlfriend to transfer this amount to his bank in New York, telling her he wanted to play a joke on a computer operator friend who worked at the bank. The friend and the money disappeared before the girlfriend realised she had been deceived as well as jilted! [19]

The list of such cases would be amusing if the problem were not so serious. Various commentators estimate that only 1% of computer crimes are detected. It is difficult to see how anyone can estimate a percentage of that which is itself unknown. But whatever the figure, it is clear that the cases detected represent only the tip of the ice berg.

Estimates have been given in the United States that no more than 15% of the people caught out in computer crimes are ever reported to police.[20] Reasons are offered for this:

* embarrassment at the discovery of crime on the part of trusted personnel in highly responsible positions;
* fear lest publicity about large scale crime should damage confidence in the corporation and do disproportionate damage;
* the typical popularity and admiration for many in-house computer criminals who frequently turn out to the anything but the stereotype of the criminal in the popular mind. In the book Crime to Computer Donn Parker describes them 'perpetrators are usually bright, eager, highly 'motivated, courageous, adventuresome and qualified people willing to accept the technical challenge. They have exactly the characteristics that makes them highly desirable employees in data processing.[21]

More analysis suggests that this picture may itself be a stereotype. Environment, not personality, may be the chief factor in promoting wrongful conduct on the part of people, usually trusted people, having access to computers. In the absence of adequate security gateways and audit checks, the perception of the ease and speed with which money can be moved around, provides the temptation that may turn decent citizens into computer criminals.

The problem of computer crime detection is one of hauling police methodology into the informatics age. To some extent, computers themselves come to the aid of detection. The technique of 'matching' different computer tapes to detect inconsistencies,

errors, questionable transactions and so on is already well developed in Australia. It has been used, quite successfully, for example to detect manipulation of the social security computer by officers of that Department. This has led to their prosecution and conviction in a number of cases.

It is now well known that the Royal Commission of Enquiry into the Ship Painters' and Dockers' Union in Victoria (the Costigan Commission) had installed a most sophisticated range of computer equipment to collect, analyse and compare data from the huge number of witnesses and documents being examined by the enquiry. By matching techniques, information supplied from many sources can be compared, contrasted, placed in chronological order and otherwise analysed for consistency with other material and probability of truth or error.

The Assistant Director of the Australian Bureau of Criminal Intelligence, Mr. Wal Williams, said in October 1982 that, from the point of view of criminal intelligence 100 clerks could not do the work now being done by a good police computer. The head of the Federal Police Planning and Research Branch, Chief Inspector L.J. CLaydon, was reported as saying:

> If you got a truck load of documents, company records and financial statements you would need 10 to 15 years to examine them and make some inference of organised crime. The computer allows us to analyse the information rapidly so police can identify associations which are virtually impossible to do manually.[22]

In December 1982 it was announced that new computer training course for police and corporate affairs officers in New South Wales would be established in 1983 to tackle sophisticated computer and corporate crimes. The course is to be open to police and Corporate Affairs Commission officers in all States. Its establishment followed discussion at the Australian Police Ministers' Council[23], as reported the course will be operating in mid-1983. About 11 police and 11 CAC officers will attend each course. Detective Sergeant Ron Armstrong of the N.S.W. Fraud Squad commented that computer-related crime was on the increase. A recent study had suggested that about 4,000 computer frauds involving about $200 million had been committed since 1974. Sergeant Armstrong expressed the opinion that computer crime was no different to any other fraud apart from its speed and facility and the ease with which it could be hidden. Among the skills police would have to learn was how to close a computer to protect evidence for use in the trial. They would also have to know how to prevent remote terminals from interferring with information stored on the computer in order to destroy evidence, delay police or cover the track of criminals.[24]

All thinking members of the community in Australia will be pleased to see that the police are developing expertise in relation to computer crime. But will enough police be involved? Will the training keep up with the technology? How can we equip a career police service, often undermanned and ill paid, to keep pace with the skills and techniques of the computerist elite of the technological society? This is a matter which should have the highest priority attention of police administrators and politicians.

COMPUTER CRIME: EVIDENCE AT THE TRIAL

There will be little effective protection for society if, despite all the odds, a computer criminal is found, reported, charged and prosecuted in court but the laws of evidence we follow unjustly stand in the way of the proof of computer transactions or if otherwise such transactions cannot be established 'beyond reasonable doubt' to the satisfaction of the court or jury.

A major enquiry presently being undertaken by the Australian Law Reform Commission involves a review of the Federal laws of evidence in Australia. The basic problem facing us is the strong tradition of the continuous oral trial which is at the heart of the Australian criminal trial system. Although it is more efficient to make decisions on the basis of documentary evidence (for documents can be read four times faster than the same evidence can be given orally), our court system, unlike that of Europe has long resisted documents. It has had an eight centuries infatuation with oral testimony. The hearsay rule, the best evidence rule and other principles frequently prevent the production of documentary evidence. This results in witnesses being called, whose evidence can be tested by cross-examination and whose demeanour can be scrutinised by the parties, the judge, magistrate or jury. With the advent of the computer, this rule becomes very inconvenient. The whole point of computerisation may be to get away from the expensive proof of original transactions by many hands. It is for this reason, and because computers are overwhelmingly reliable, that the laws of evidence have been changed in all Australian jurisdictions to permit the admission into evidence of computer material.

Unfortunately, the legislation that has been enacted in Australia on this subject has all too frequently lagged behind technological developments already in place at the time the remedial legislation was passed. For example, legislation enacted to permit the admission of microfilm into evidence in courts does not, typically, apply to laser technology which has been adopted since the laws were passed. Another case arises from the use of 'on line' computers by bank customers such as is now becoming common in Australia with 'automatic tellers'. Even under the broadest of Australian evidence reform

legislation, entries made by customers in effecting transactions at 'automatic tellers' may not qualify for admissibility in court under Federal or N.S.W. legislation. Typically, this legislation requires that, to be subsequently admissible in a court of law, information must be recorded in computer records of a business by a 'qualified person'. It is doubtful whether a customer at an automatic teller could be described as a 'qualified person'. The phrase probably was intended to be limited to trained and therefore reliable operators. Likewise, computer-generated evidence (which is produced without any imminent human intervention) is not admissible under any of the technological evidence legislation in some Australian jurisdictions, though it may be admissible at common law, provided normal rules governing evidence produced by a machine can be satisfied.[25]

These are just a few examples of the problems which law reform faces in seeking, by highly specific means, to confront the new technology. All too often the technology outstrips the legislation. The technologists would laugh at the feeble efforts of lawyers and law makers to keep pace, if the consequences were not so serious. It is vital that the laws of evidence be reformed keeping in mind the fact that computers can produce mistakes, whether through negligence or deliberate intervention, technical faults or otherwise. But it is also vital that courts of law should keep pace with technological development so that the decision maker (judge, magistrate or jury) is not deprived of vital and reliable evidence by antique rules which were developed long before computication changed the base of information, on which the world's decisions are now made.

COMPUTER CRIME: PUNISHMENT

Even if the gateways are passed and the hurdles overcome of substantive law, reportage, detection and proof, it is essential that our punishments for criminal conduct should be reviewed to take into account the specially anti-social consequences which computer crime and disruption can sometimes cause. In a sense, this is another example of the problem caused by trying to push new conduct into categories designed for earlier times. The already high and growing dependence of society on computerised information makes our community increasingly vulnerable to destruction of or interference with that information. Yet an offence of 'malicious injury' to property may carry a relatively light penalty, quite insignificant as a deterrent against the major social and economic dislocation that could be caused by damage to a computer facility, computer tape or the like. An American commentator put it thus:

> Theft of services is only a misdemeanour in New York, the maximum punishment is a year in gaol. Where there has been a significant loss, perhaps as much as $200,000...the deterrent value of a misdemeanour is questionable...The law really hasn't come to grips with the problem of classifying theft of intangible things such as computer time or storage...Often a specific statute like theft of services is interpreted to preclude the application of a more general statute such as larceny.[26]

We have similar problems in Australia. Sometimes the available penalty may be entirely appropriate for the computer criminal. But the potential of computer crime to involve massive amounts of money, to cost enormous sums in detection and proof and to disrupt large numbers of corporations and peaceful citizens dependent on the computing resource, all suggest that a review of punishments for computer crime is appropriate. Such a review could best be done in the context of an examination of the modern definition of computer crime and the assignment of appropriate maximum punishments for identified anti-social conduct. Whether punishment in penal theory is based on deterrence, retributions, rehabilitation or a combination of these and other considerations, it is plain that punishments assigned in earlier times for different criminal conduct (without the ripple effect typically attaching to computer crime) may just not fit the appropriate penalty for today's technological criminal. Our crimes are out of joint. And they are so very largely because an amazing new technology, with large potential for good and a huge potential for wrongdoing is now with us and rapidly penetrating our community. Criminal law, police detection, the trial process, the laws of evidence, the constitution of the courts and the available punishments have not kept pace with the informatics revolution.

CONCLUSION

The chief point of this contribution is that there is an urgent need for consideration of the social and legal implications of computerisation of our society. Computer crime and its implications for the criminal law and policing, locally, nationally and internationally represents only one part of the mosaic that must be put in place as society responds to informatics. The chief point I want to make is that there is insufficient attention being given and that there is an insufficient sense of urgency about the need to give such attention to these problems.

Within Australia, the constitution did not assign the criminal law to the Federal Parliament, as occurred when the Canadian Federation was established. Crime has overwhelmingly remained State business in Australia. There are Federal crimes and there is a Federal Police: but they represent only a small proportion of the criminal docket, so far.

Computers, linked by telecommunications, are indifferent to the colonial borders which divide the continent of Australia. Indeed, in many respects as cases which have already occurred will demonstrate, they are indifferent to international borders through trans border data flows. Crime, its policing and punishment are traditionally and legally bound to a particular jurisdiction. The road ahead for Australia must shortly be chosen in respect of computer crime. Are we with this national and international technology to stick with the old colonial borders, defining computer crime and providing for its detection and proof differently in one part of the country when compared to another? Would this provide yet another obstacle to an effective social response against criminal conduct utilising computers? Will our law enforcement agencies be faced by barren legal argument, in cases having an interstate or international component, that the crime complained of is beyond the particular jurisdiction of the State court in which it was charged? Will the differing rules of evidence in different States provide barriers against the ready proof of computer crime and loopholes through which these criminals, almost by definition intelligent and often well-heeled from the wrong-doing, can escape?

There is in the Australian Constitution power in the Federal Parliament to make laws with respect to telecommunications and matters incidental to that power. The growing integration of computers and telecommunications, the so-called 'computications' revolution which has occurred in the 1970's, may provide us in Australia with a solution to what promises to be an important national problem. Should the power of the Commonwealth Parliament over telecommunications be used as a basis for defining, detecting, proving and punishing computer crime in Australia, insofar as that crime involves the use of telecommunications? That is an important issue for the decade ahead.

Some will see this suggestion as a threat to established State areas of concern in the criminal law. Some will see it as a danger to established police interests, bureaucratic empires, personal careers. It is not meant to be so. I suspect that unless we can find effective national laws on computer crime, or mutually supportive and compatible State laws on the subject, the sophisticated computer criminals of the future will laugh all their way to and from the bank, able to manipulate our criminal justice system because, in the age of satellites, trans border data flows and computications Australia adhered to an insistence on borders many of them drawn accidentally by long forgotten and unremembered officials in the Colonial Office. True, the small league will be caught. But the big league of computer criminals will be able to manipulate such insufficient laws. And we must not let that happen.

I cannot tell whether the Federal Attorney-General will give a reference on this task to the Law Reform Commission. The proposal is under consideration. But I repeat. Whether it is the Law Reform Commission or some other body that examines the local and national implications of computer crime in all its facets, there is an urgent need for such an examination so that our laws can be set in place to defend society against the computer criminal. It will be a poor commentary on our criminal justice system if in the 21st century, it can be said that we provided splendid laws and police services to deal with shoplifting, petty crime and street disturbance but failed adequately to consider and address the big anti-social problems of our time.

FOOTNOTES

1. Question by Mr. R. Jacobi, M.P., Commonwealth Parliamentary Debates (House of Representatives) 9 November, 1982, 2935.

2. Organisation for Economic Co-operation and Development, Guidelines Governing the Protection of Privacy in Trans Border Flows and Personal Data, see (80) 58. The Guidelines are reproduced in Transnational Data Report. Vol 4 No 1 (January 1981) 45.

3. Australian Law Reform Commission, Reform of Evidence Law, Discussion Paper No. 16 (ALRC DP 16), 1980.

4. See National Crimes Commission Act 1982 (Cwlth).

5. K.E. Brown, 'Towards an International Convention of Computer Related Crime', mimeo, Victoria Police Fraud Squad, 1982.

6. Ward v. The Superior Court of California 3 CLSR 206 (Cal) (1972).

7. U.S. District Court for the District of Maryland, Crim No. 76-079H. Cf Hancock v. Decker 379 F 2nd 552 (1967). Discussed in J. Bing, 'Information Law?' in (1981) 2 Journal of Media Law and Practice 219.

8. P. Robinson, 'Legal Questions and Trans Border Data Flow', paper for the Swedish and Norwegian Society for Computers and Law, January 1982, mimeo, 4.

9. The Law Commission (Eng.) WP 56, Conspiracy to Defraud, 1974. See also J.R. Sulan, 'Legal Aspects of Computer Crime: Is the Law Adequate?' Forum (1980) Vol 3 No 4 p 37. 'Computer Abuse: A Fact of Life in Australia' in Transnational Data Report, Vol 4 No. 1 (1981), 27.

10. Brown, Appendix A.

11. Treacy v. Director of Public Prosecutions [1971] AC 537 (HL).

12. Director of Public Prosecutions v. Stonehouse [1978] AC 55 (HL).

13. Henderson and Young, 'The $10 Million Theft That Nobody Noticed', Readers' Digest, October 1981, 66.

14. Brown, 1-2.

15. Case cited in J. Bloom Becker, 'How to Recognise the Computer Criminal' in Information Age, Vol 4 No 4, October 1982, 194, 198.

16. ibid, 198.

17. ibid, 196.

18. id, 196.

19. id, 199.

20. Bloom Becker, 196 citing D. Parker.

21. D. Parker, Crime by Computer cited by Bloom Becker, 197.

22. The Age, 29 October 1982.

23. Sydney Morning Herald, 8 December 1982.

24. ibid.

25. Cf The Queen v. Weatherall (1981) 27 SASR 238. See generally T.H. Smith 'Legality - Information Technology and the Law of Evidence' (1982) 1 Jl. Law and Info Science 89.

26. Bloom Becker, 195.