Parliamentary Joint Committee on the National Crime Authority

THE LAW ENFORCEMENT IMPLICATIONS OF NEW TECHNOLOGY

AUGUST 2001

Parliament of the Commonwealth of Australia

THE LAW ENFORCEMENT IMPLICATIONS OF NEW TECHNOLOGY

A report by the Parliamentary Joint Committee on the National Crime Authority

AUGUST 2001

ISBN 0 642 71150 X

This document was produced from camera ready copy and printed by the Department of the Senate Printing Unit, Parliament House, Canberra.

MEMBERSHIP OF COMMITTEE

Hon Bruce Baird MP, Chairman*

Senator George Campbell, Deputy Chairman

Senator Kay Denman

Hon Graham Edwards, MP

Senator Jeannie Ferris

Senator Brian Greig

Mr Gary Hardgrave, MP

Hon Duncan Kerr, MP

Senator Julian McGauran

Mr Alby Schultz, MP

* Mr Peter Nugent MP was Committee Chairman until his death on 24 April 2001. Mr Baird was elected Chairman on 24 May 2001.

Secretariat:

Mr Michael McLean, Secretary
Ms Barbara Allan, Senior Research Officer

DUTIES OF THE COMMITTEE

The *National Crime Authority Act 1984* provides:

55. (1) The duties of the Committee are:

(a) to monitor and to review the performance by the Authority of its functions;

(b) to report to both Houses of the Parliament, with such comments as it thinks fit, upon any matter appertaining to the Authority or connected with the performance of its functions to which, in the opinion of the Committee, the attention of the Parliament should be directed;

(c) to examine each annual report of the Authority and report to the Parliament on any matter appearing in, or arising out of any such annual report;

(d) to examine trends and changes in criminal activities, practices and methods and report to both Houses of the Parliament any change which the Committee thinks desirable to the functions, structure, powers and procedures of the Authority; and

(e) to inquire into any question in connection with its duties which is referred to it by either House of the Parliament, and to report to that House upon that question.

(2) Nothing in this Part authorises the Committee:

(a) to investigate a matter relating to a relevant criminal activity; or

(b) to reconsider the findings of the Authority in relation to a particular investigation.

TABLE OF CONTENTS

RECOMMENDATIONS

Recommendation 1: That the Government give consideration to the range of offences prescribed under sections 5(1) and 5D of the *Telecommunications (Interception) Act 1979* in the context of contemporary technological developments (para. 1.41).

Recommendation 2: That the Government make TI-related foreign intelligence warrants available to law enforcement agencies (para. 1.41).

Recommendation 3: That the Commonwealth consult with the Standing Committee of Attorneys-General whether regulation of the use of TI could be delegated to the States and Territories within a continuing context of broad-based mirror legislation (para. 1.55).

Recommendation 4: That the Government give particular consideration to the appropriate level of regulation of Internet Service Providers to ensure their cooperation with law enforcement (para. 1.73).

Recommendation 5: That the Government ensure that the integrity of the TI Act is not undermined by emerging technology (para. 1.79).

Recommendation 6: That, in conjunction with the States, the Government introduce comprehensive national electronic surveillance legislation, with particular emphasis on the inclusion of appropriate privacy provisions (para. 1.116).

Recommendation 7: That the Australian Government place on the agenda of the Standing Committee of Attorneys-General the need for a comprehensive and fundamental review of the operations of legislative provisions that may inadvertently and unnecessarily restrict the capacity of law enforcement to exchange intelligence and operational information (para. 1.124).

Recommendation 8: That the Commonwealth Ombudsman's jurisdiction over the use by Commonwealth law enforcement agencies of telecommunications interception be expanded to include the use of any electronic surveillance device (para. 1.158).

Recommendation 9: That a national cyber-forensic facility be established (para. 2.145).

ACRONYMS

ABCI	Australian Bureau of Criminal Intelligence
ABN-DSC	Australian Business Number Digital Signature Certificate
ACCC	Australian Competition and Consumer Commission
ACID	Australian Criminal Intelligence Database
ACS	Australian Customs Service
AFP	Australian Federal Police
AGEC	Action Group on the Law Enforcement Implications of Electronic Commerce
AIC	Australian Institute of Criminology
AIIA	Australian Information Industry Association
ALEIN	Australian Law Enforcement Intelligence Net
APG	Asia-Pacific Group on Money Laundering
AUSTRAC	Australian Transaction Reports and Analysis Centre
CCR	Call Charge Record
CJC	Criminal Justice Commission (Queensland)
CoE	Council of Europe
DFAT	Department of Foreign Affairs and Trade
DPP	Director of Public Prosecutions
ECEG	Electronic Commerce Expert Group
ECTF	Electronic Commerce Task Force
EU	European Union
FATF	Financial Action Task Force
FTR Act	*Financial Transaction Reports Act 1988* (Cth)
ICAC	Independent Commission Against Corruption (NSW)
ISP	Internet Service Provider
MCCOC	Model Criminal Code Officers Committee
NAFIS	National Automated Fingerprint Identification System
NCA	National Crime Authority
NCA Act	*National Crime Authority Act 1984* (Cth)

NOIE	National Office for the Information Economy
NSWCC	New South Wales Crime Commission
OECD	Organisation for Economic Cooperation and Development
OSCA	Office of Strategic Crime Assessments
POC Act	*Proceeds of Crime Act 1987* (Cth)
QCC	Queensland Crime Commission
RGEC	Research Group on the Law Enforcement Implications of Electronic Commerce
SMS	Short Messaging System
TI Act	*Telecommunications (Interception) Act 1979*
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law

PREFACE

Background

At a private meeting on 29 June 2000 the Committee gave consideration to the increasing amount of evidence that emerging technology, most particularly in the communications and information fields, was playing an ever more pervasive role in both criminal behaviour and law enforcement activity. It had been maintaining a general watching brief on the topic during the preceding three years as a result of its predecessor Committee in the 38th Parliament having conducted a public hearing on 24 March 1997 with three leading experts specifically into the electronic commerce dimension of the issue.[1] That Committee had also conducted a public hearing in December 1996 with the then Secretary General of Interpol, Mr Raymond Kendall, at which the globalisation of crime using modern communications systems had been one of the issues discussed.[2]

The information technologies then under discussion were considered to be in a state of relative infancy and, given the speed of change in the world of high technology, prediction of the shape of future events and how governments should respond were problematic concepts. Much of the discussion was necessarily speculative and the witnesses cautioned against hasty regulatory responses while the state of knowledge about the nature and extent of problems was limited. It was noted that the same technologies that law enforcement views as having some potential problems may, in time, present solutions to these problems. The then Committee had been both assured and reassured that appropriate attention was being paid by Australian Government authorities to the law enforcement implications of electronic commerce and it had not further pursued the issue. It was satisfied that its members had been able to gain a better understanding of the issues and, through the conduct of the hearing in public, it had made a contribution to a more informed public debate.

The following extracts give some indication of the context to the Committee's discussions when it again came to consider the impact of new technology on law enforcement in June 2000. The extracts are a mere sample of the vast amount of discussion in the community of the challenge that new technology is seen as representing.

---

1 The transcript of the hearing can be accessed through http://www.aph.gov.au/nca

2 For details see the Committee's February 1997 report entitled *Law Enforcement in Australia - An International Perspective.*

Director of the Australian Institute of Criminology (AIC), Dr Adam Graycar, wrote the following introduction to the Institute's January 1998 Trends and Issues paper entitled *Technology and Crime Control* by then AIC Deputy Director, Dr Peter Grabosky:

> As we approach the 21st century, our efforts to tackle the challenge of crime will be assisted significantly by developments in technology. From improvements in locking and alarm systems, to new devices for location, identification, and surveillance, to means of restraining individuals who pose a risk to themselves or others, the crime control tasks confronting both the community and our police services will be made easier. Technology can assist us in making optimal use of finite resources.
>
> Along with these new technologies, however, come certain downside risks. Some systems are vulnerable to excessive or inappropriate use, while others may have unintended adverse consequences, such as potential for harm to third parties. This Trends and Issues paper reviews some of the emerging technologies which may be applied to crime control. Recognising that new technologies should not be embraced uncritically, it discusses some of the principles which might accompany their introduction in a democratic society.[3]

Dr Grabosky's paper had carried the following cautionary words:

> The development and deployment of crime control technology should be based on thorough consultation. To do less would run the risk of bringing the entire criminal justice system into disrepute…It is not sufficient to assume that new technologies of crime control will automatically lend themselves to responsible use.[4]

In the May 1997 report of the Royal Commission into the NSW Police Service, Commissioner Justice James Wood had addressed the topic from the viewpoint of the efficiency and effectiveness of law enforcement. In his conclusions to the chapter entitled *Integrity Measures (I) Criminal Investigations* he wrote:

> The law has lagged well behind technical developments and patterns of crime…Yet [despite a number of representations and submissions to Government] substantial problems and uncertainties persist. If law and order are serious issues on the political agenda, then the matters outlined in this section of the Report require careful consideration and implementation, rather than endless debate and procrastination.[5]

---

3 Included in *Submissions to Parliamentary Joint Commission on the National Crime Authority, The Law Enforcement Implications of New Technology,* [hereafter *Submissions*], p. 2.

4 Included in *Submissions*, p. 6.

5 Royal Commission report p. 460, included in *Submissions,* p. 106.

Similarly, then NCA Chairperson, Mr John Broome had said in October 1998 in a paper entitled *Electronic Surveillance in Criminal Investigations: Balancing Law Enforcement with Civil Liberties*:

> …the real problem with telephone interception is that the law has not kept pace with technology. For years we have been hidebound to 1970s technology, notwithstanding the advent first of analogue and then of digital mobile telephones. …technology is changing so rapidly that the kinds of electronic surveillance which are appropriate today may be totally outdated tomorrow. Australia's experience in telephone interception is a case study in why we should not legislate in relation to technology but rather in relation to the activity involved. The Telecommunications Interception Act is essentially based on the technology of the handset…The world moved on and the Act stayed fixed in time.

Mr Broome also stated at the Australian Institute of Criminology's conference on *Transnational Crime* in March 2000 that:

> The kinds of criminal activities that we now talk about as organised or transnational crime are very serious… But whether these crimes occur at the national or transnational level they are, conceptually at least, capable of investigation, prosecution and conviction, **provided we are armed with the necessary weapons** [emphasis added]… The success of transnational crime has more to do with the capacity in law enforcement agencies than the organised skill of the transnational criminals.

In November 1999 the Parliament amended the *Australian Security Intelligence Organisation Act 1979* to modernise ASIO's powers to enable it to meet the challenges posed by new technology in its fight against the *terrorist threat* to Australia, including the use of contemporary surveillance technologies.[6] This raised in the Committee's mind the question of whether such provisions should be extended to law enforcement agencies such as the NCA, which have to address the national and transnational *criminal threat* to Australia.

Finally, at the March 2000 meeting of the Conference of Police Commissioners of Australasia and the South West Pacific Region - with the theme of 'Crime @ the speed of thought' - the Commissioners agreed to establish an Electronic Crime Steering Committee because of their recognition of the real potential for global criminal exploitation of new and emerging technologies and cross-jurisdictional differences.

Accordingly, the Committee felt that it was appropriate and timely that it should conduct a broad examination of the law enforcement implications of new technology. While it was clear that the nature of the problems confronting law enforcement was well recognised, the Committee saw it as desirable that there was an opportunity for public discussion over the need to weigh the demands of law enforcement agencies

---

6 *Australian Security Intelligence Organisation Legislation Amendment Act 1999.*

like the NCA for access to the latest technological tools against the community's proper concerns about the balancing of human rights and privacy considerations.

Terms of reference

The Committee adopted the following terms of reference for its inquiry:

> The Committee will inquire into the law enforcement implications of new technology, with particular reference to:
>
> (a) whether use of new technology by law enforcement agencies is adequately catered for by Commonwealth, State and Territory legislation;
>
> (b) the extent to which electronic commerce facilitates the laundering of the proceeds of crime; and
>
> (c) whether international law enforcement cooperation is adequate to meet the challenges of new technology.

At the time, the Committee's then Chairman, Mr Peter Nugent MP, announced its inquiry with the following statement:

> The Committee is aware of mounting concern about the capacity of law enforcement to prevent criminals from using new technologies to their advantage. Agencies like the NCA have warned that technology opens up a whole range of new opportunities for criminals. That same technology may, however, hold the key to improved policing. The Committee therefore proposes to conduct a comprehensive inquiry into the implications of new technologies for law enforcement. In particular, the Committee wants to determine whether the legislative regime underpinning agencies like the NCA supports their efforts to both combat technology-related crime and to maximise the use of technology in pursuing offenders.[7]

The inquiry is conducted pursuant to paragraph 55(1)(d) of the *National Crime Authority Act 1984* which places on the Committee the duty to examine trends and changes in criminal activities, practices and methods and to report to both Houses of the Parliament any change which it thinks desirable to the functions, structure, powers and procedures of the Authority.

Conduct of inquiry

The Committee's inquiry was advertised in the national press in July 2000. The Committee received 28 submissions, two of which were accorded confidential status. Details of submitters are shown in Appendix 1.

---

7 Media Release *Parliamentary Committee to Inquire into New Technology and Law Enforcement,* 29 June 2000.

In lieu of a submission, then AFP Commissioner M J Palmer, in his capacity as Chair of the Police Commissioners' Conference Electronic Crime Steering Committee, provided the Committee with a copy of *The Virtual Horizon: Meeting the Law Enforcement Challenges*, a comprehensive scoping paper for developing an Australasian law enforcement strategy for dealing with electronic crime. This report published through the Australasian Centre for Policing Research, and a second ACPR report entitled *Technology Environment Scan* which was provided to the Committee by the Centre's Director, Commander Barbara Etter, proved invaluable to the Committee's consideration of the electronic crime issue.

Private correspondence was also exchanged with the US Federal Bureau of Investigation, the European Commission and the Hong Kong Police Force, as the Committee sought to gain an international perspective on issues of common interest.

Five public hearings were conducted over the period November 2000 to April 2001, details of which are set out in Appendix 2. Evidence was also taken in camera. While this evidence is not expressly cited in this report, it contributed to the Committee's understanding of the issues.

In October 2000 the Committee undertook an inspection of the Australian Federal Police Forensic Services Centre in Weston, ACT, and was shown demonstrations of fingerprint enhancement technologies, the forensic biology and DNA laboratory, and the forensic chemistry/criminalistics laboratory. The Committee expresses its thanks to the Centre's Director, Dr James Robertson, and his expert and enthusiastic team for their contributions to an informative and worthwhile visit.

Further, in November 2000 the Committee's secretariat was provided with a comprehensive briefing on the operations of the Australian Bureau of Criminal Intelligence (ABCI) at its Canberra offices by its then Director, Mr John Ure, and several of his senior personnel. The Committee has had the benefit of the briefing material provided to its staff. It also looks forward to taking up the offer of current Director, Dr Grant Wardlaw, to making a similar visit. A brief description of the operations of the ABCI is included in Chapter 1.

The report

This report addresses each of the Committee's terms of reference in a separate chapter, which has proven to be a convenient basis for discussion of the myriad issues raised by the topic. Chapter 1 essentially addresses the legislative situation in Australia relating to the capacity of law enforcement to have access to new technologies to enable it to respond effectively to contemporary crime. It is with some disappointment that the Committee notes that, with major organised crime groups now operating on a national and transnational basis, Australian policing still seems to be hamstrung by an inability to agree to a nationally consistent approach to multi-jurisdictional investigations. While it is convenient to lay blame on the anachronistic nature of the Constitution in this respect, the Committee emphasises its belief that cooperation between the tiers of government - and between national governments - holds the key to future law enforcement success.

Chapter 2 broadly addresses the potential for money laundering via the relatively new medium of electronic commerce. The increasing development of 'cyberspace', and the use of the Internet to communicate therein, has already led the Australian Government to introduce several pieces of legislation not only to seek to facilitate electronic commerce,[8] but also to address some of the downsides of the growth of the Internet, including in relation to restricting access to certain categories of offensive material[9] and online gambling.[10] In this Chapter the Committee discusses the features of electronic commerce and its possible use by criminals to launder money.

In Chapter 3 the Committee seeks to determine the extent to which the international community is addressing the increasingly global dimension of law enforcement and comments on the adequacy of Australia's role within that debate.

In the course of its inquiry the Committee has learnt that there is a very considerable amount of discussion about new technology and law enforcement on the public record. Much of that material addresses the role of new technology in the detection and avoidance of traditional State-based crime, such as traffic offences and burglary. In order to keep within its statutory parameter of examining the NCA's role and functions, the Committee has concentrated in this report only on issues primarily relating to national and transnational criminality.

Another area raised with the Committee was the need for the enactment of a range of new offences to counter the use of computers to commit crimes. The NCA informed the Committee that it is restricted to investigating only those technology-related offences that fit established offence categories, such as theft or fraud.[11] The Attorney-General's Department nominated the following as a non-exhaustive list of e-crimes:

> …intellectual property theft, denial of service attacks, child pornography, fraud, virus propagation, spamming, the dissemination of offensive materials, commercial espionage, sabotage, electronic terrorism, cyber stalking, tax evasion and money laundering.[12]

While the Committee addresses the question of the extension of the NCA's powers to access new technology in pursuit of its goals, the Committee has not gone into detail about the possible content of computer offences legislation in this report. To do so would duplicate the activities of the Model Criminal Code Officers Committee (MCCOC), which in January 2001 published a 354-page report on this topic entitled *Damage and Computer Offences.*

---

8 *Electronic Transactions Act 1999.*

9 *Broadcasting Services Amendment (Online Services) Act 1999.*

10 *Interactive Gambling Act 2001.*

11 *Submissions*, p. 149.

12 *Hansard Transcript of Evidence,* Joint Committee on the National Crime Authority, [hereafter *Evidence*], p. 26.

In his letter of transmittal of the report to contributors, MCCOC Chair, Justice R. N. Howie, wrote:

> The computer offences are of course very important and topical. The Committee believes that it is critical that offences exist which are appropriate to the current technological environment and that there be a consistent approach to the nature and scope of such offences adopted throughout Australia. Operations and transactions involving computers have no regard to jurisdictional boundaries.

This Committee endorses Justice Howie's sentiments and congratulates his team for their comprehensive analysis of the issues and the emphasis placed on the need for a common approach across jurisdictions. However, in the full knowledge that consideration of this issue is current, the Committee adopted terms of reference which sought to avoid direct duplication of the MCCOC's efforts.[13]

Acknowledgments

The Committee records with deep regret the death of its former Chairman, Mr Peter Nugent MP, during the course of this inquiry. He made a substantial contribution to the Committee's work and his efforts were clearly appreciated by the NCA and its law enforcement partners.

The Committee wishes to express its appreciation to all parties who made a contribution to the conduct of this inquiry, whether by making a written submission, by personal attendance at a hearing or, in many cases, by both written and oral submissions. While all witnesses were personally thanked by Mr Nugent at the time of their giving evidence, he made a particular reference to the contribution of the officers of the Attorney-General's portfolio when they appeared before the Committee at the public hearing held on 4 December 2000. The portfolio's 64-page submission is a comprehensive and authoritative statement of the challenges and opportunities that lie ahead.

The Committee also wishes to recognise the efforts of the officers of the secretariat who assisted it with the conduct of this inquiry and the drafting of this report.

Bruce Baird MP
Chairman

---

13 On 27 June 2001 the Government introduced the Cybercrime Bill 2001 into the House of Representatives. On 28 June 2001 the Senate referred the Bill to its Legal and Constitutional Legislation Committee. That inquiry was continuing at the time of the preparation of this report.

CHAPTER 1

THE ADEQUACY OF THE AUSTRALIAN LEGISLATIVE STRUCTURE

Introduction

1.1 The use of technology in pursuit of crime control has a long history. For example, English criminologist Edward Henry is credited with creating the first set of fingerprint records in 1901, exactly 100 years ago.[1] As will be discussed in detail below, through electronic, laser and information technology developments, fingerprint records are now available to all Australian police services for instantaneous cross-matching purposes. Such rapid access to information is, of course, a major bonus to effective policing where speed of response is critical.

1.2 While the range and sophistication of the forensic sciences has continued to develop over the past century, with DNA matching the most prominent contemporary example, recent growth of technology has been described as 'exponential and rapid'.[2] It is clear that initiatives in the forensic and related sciences, combined with developments in computer technology and in other technological areas, such as the invention of drug- and explosives-detecting ionscan machines, have come to play a prominent role in law enforcement's armoury and that their results have made a significant contribution in the pursuit of successful prosecutions.

1.3 Further, while many of the more sophisticated tools are not inexpensive, many others have become available at ever diminishing cost and provide quicker results, thus increasing their overall value to law enforcement. As operating environments become increasingly cost-conscious, especially in the public sector, greater reliance will be placed on technology rather than human resources for achieving ever-higher productivity at ever-lower costs. It is apparent that, while there will always be a role for traditional labour-intensive policing methods, they will be increasingly supplemented and complemented by technological aids.

1.4 The keys to the past successes of technology in law enforcement have been several, but two considerations in particular stand out for mention: the level of legislative recognition which has been given to their use and the extent of acceptance by the courts of evidence generated by technical means. Without statutory recognition, the collection of such evidence by law enforcement risks being declared inadmissible by the courts - with the result that the prosecution case may collapse. When backed with proper legislative support, such evidence is often sufficiently

---

1 See http://library.thinkquest.org

2 *Evidence*, p. 1.

irrefutable to encourage an early guilty plea, with the accompanying benefits to prosecution and court processes.

1.5 In this Chapter, the Committee will seek to assess the extent to which the Commonwealth, State and Territory governments have ensured that the legislative regimes within their respective jurisdictions which underpin the NCA's operations are keeping pace with emerging technologies. It should be borne in mind that the NCA's role is essentially to combat national complex organised crime. While it is a creature of Commonwealth statute, its status is recognised and its operations underpinned by complementary legislation in each State and Territory. It is the only law enforcement agency in Australia whose investigations are not limited by jurisdictional boundaries.

1.6 There is clearly an extensive and ever-growing range of technological aids available to the general community for crime avoidance and to law enforcement for crime control. The Australian Institute of Criminology's 1998 Trends and Issues paper entitled *Technology & Crime Control,* included as part of the AIC's submission to this inquiry, discusses many in impressive detail.[3] There is also no apparent shortage of devices available to the better-resourced criminals with which to seek to thwart the efforts of their pursuers. The submission of the Australian Bureau of Criminal Intelligence referred to the case of Brendan Abbott, the so-called 'Postcard Bandit':

> When apprehended, Abbott had access to not only firearms but also police radio frequency scanners, electronic lock picking devices, information on constructing electronic devices including listening devices, mobile phone SIM-cards, software and computer hardware to produce counterfeit identity documents, as well as a number of false documents including drivers licences.[4]

1.7 As noted in the Preface, in this report the Committee will only address the major technological issues with a *national* crime perspective - to also include *community* policing issues would be too extensive a topic for this inquiry and would also stray beyond the Committee's primary area of interest.

1.8 Several submitters noted that there are currently inadequacies and inconsistencies in the frameworks of the several Australian legislatures to cater for technological change and to enable law enforcement to combat emerging technological crimes. The Australian Federal Police (AFP), for example, noted that '[c]urrent legislation was enacted whilst these things [police access to information, people and places] were predominantly physical. Now, however, these things exist in cyberspace. Current legislation is not adequate because it is silent on law enforcement use of new technologies'.[5] It was also pointed out by the Australian Information

---

3 *Submissions,* pp. 2-6.

4 *Submissions*, p. 128.

5 *Submissions,* p. 61.

Industry Association (AIIA) that, despite the similarities in the nature of the offences committed, the major difference between off-line offences and their online equivalents is the absence of the physical element.[6]

1.9 Stress has also been placed on the inter-jurisdictional nature of technological crimes, especially those committed by organised crime groups. Computer-related crimes in particular represent a serious challenge to the current approach to law enforcement based on national and State/Territory boundaries. While one discussion point in this inquiry has been the continuing relevance of the current national system of law enforcement to this 'borderless' environment, the Committee believes that the key issue for its consideration in the context of this inquiry is the extent to which the Parliaments in whose jurisdictions the NCA is expected to operate are *unnecessarily* constraining its access to the use of new technologies in its fight against organised crime. The Committee is mindful that use of some of the emerging technologies for crime control carry downside risks, not least from human rights and privacy perspectives, and that these factors need to be carefully weighed before proposals are advanced which would expand the range of NCA tools and powers.

1.10 Modern policing needs to address crimes which will routinely cross domestic and international jurisdictions. While Chapters 2 and 3 deal with the national and international dimensions of electronic crime, in this Chapter the Committee looks at the new technology challenges for policing primarily within Australia, especially within the Federal system where the States and Territories have responsibility for addressing the vast majority of criminality.[7]

1.11 New technologies are enabling law enforcement to develop and deploy a range of forensic and technical support tools in support of its traditional functions of detection, investigation and prosecution. The most concise summary of the critical role of technology in modern law enforcement was given by Dr Grant Wardlaw, Director of the Australian Bureau of Criminal Intelligence, in the following terms:

> We obviously have everyday things like word processors and spreadsheets for use in analysis and prosecution, software programs being developed that map criminal activity and that give spatial and temporal behaviour patterns as well as indicating offender behaviour, improvements in surveillance technology, including listening devices and telephone interception, mobile phones and emails helping officers to continually keep in touch, and, of course, national systems such as CrimTrac and our own intelligence and information systems.[8]

---

6 *Submissions,* p. 70.

7 At *Submissions,* p. 190, the Attorney-General's portfolio submission stated 'The extent of crime impacting on Commonwealth interests, including serious offences, is increasing even though in numerical terms the majority of crime overall is a matter for State and Territory jurisdictions.' This is a reference to the fact that, in Australia, the most voluminous incidents of criminality such as burglary, assault, traffic offences, and the like are matters for State/Territory regulation.

8 *Evidence*, p. 94.

The emphasis of this Chapter is on the extent to which the NCA is assisted in ensuring that those who commit major, serious criminal acts are able to be brought to justice by its being given access to such new technologies.[9]

Australia's legislative structure

1.12 While police access to several of the technologies mentioned by Dr Wardlaw is restricted only by resource considerations, others are subject to Commonwealth, State and Territory legislation of the nature sought to be examined by the Committee's term of reference (a). In order to provide a conceptual overview of the operations of this legislative structure, the Committee reproduces from the New South Wales Law Reform Commission's May 1997 Issues Paper entitled *Surveillance* a description of the division of responsibility, current as at 1996, of the Commonwealth and the State of New South Wales:

- The use of aural surveillance devices connected to the telephone system is governed by Commonwealth legislation: *Telecommunications (Interception) Act 1979* (Cth).

- The use of aural surveillance devices by Commonwealth agencies in the investigation of Commonwealth drug importation offences is regulated by Commonwealth law: *Customs Act 1900* (Cth) s 219A-219K.

- The use of aural surveillance devices by the Australian Federal Police in the investigation of certain non-narcotics Commonwealth offences is regulated by Commonwealth law: *Australian Federal Police Act 1979* (Cth) s 12B-12L.

- Aural surveillance devices used in New South Wales by State agencies and not connected to the telephone system are regulated by New South Wales law: *Listening Devices Act 1984.*

- Aural surveillance devices used in New South Wales by Commonwealth agencies (not including the Australian Federal Police) [Committee note: including the NCA] for offences which are not Commonwealth narcotic offences are regulated by New South Wales law: *Listening Devices Act 1984.*

- There is no regulation of visual surveillance, photography or the use of video cameras.[10]

1.13 This framework essentially holds true for each State and Territory in which the National Crime Authority operates, although there are sometimes distinct

---

9 While the Committee must, by virtue of its statutory basis, concentrate on the NCA, its comments will clearly have broad resonance across law enforcement in general.

10 Reproduced from New South Wales Law Reform Commission, *Surveillance,* Issues Paper 12, May 1997, pp. 24-25. The report cited its source as: B Schurr *Criminal Procedure (NSW)* (Loose-leaf Service, LBC Information Services, 1996) at para 8.70.

differences in the approaches of the States in dealing with those matters that fall within their jurisdictional capabilities. Subsequent to this 1996-based analysis New South Wales has, for example, enacted legislation to extend the *Listening Devices Act* to the operation of listening devices capable of tracking and video monitoring.

1.14 These crime fighting technologies will be addressed below under three main categories as follows:

- telecommunications interception;
- visual and other forms of electronic surveillance; and
- information and intelligence systems.

1.15 The discussion then briefly addresses the relationship of the laws of evidence in relation to new technology. It concludes with an examination of the accountability processes involved in access to relevant technologies by law enforcement, especially in view of the invasion of privacy involved.

Telecommunications interception

1.16 Telecommunications interception (TI) is a form of electronic surveillance in that, in broad terms, it provides a capacity to monitor people's affairs by electronic means. In this report the Committee will deal with issues arising from TI separately from the other forms of electronic surveillance (which are addressed in the next section below) because the Commonwealth is constitutionally responsible for its regulation under its head of power over '[p]ostal, telegraphic, telephonic and other like services'.[11] It exercises its powers through the *Telecommunications (Interception) Act 1979* [the TI Act].

1.17 While most State and Territory law enforcement agencies have access to TI information, both through the TI Act and their own State/Territory 'mirror' statutes, the other forms of electronic surveillance - such as the use of listening devices - are constitutionally issues for State/Territory regulation. The Commonwealth has, however, seen fit to pass specific legislation for use of these other forms of electronic surveillance by Commonwealth agencies.

1.18 Unquestionably, evidence gained by means of telecommunications interception is a vital contributing factor in successful prosecution of serious criminal offences. The 1994 report into the long term cost effectiveness of telecommunications interception by Mr Pat Barrett (at that time a Deputy Secretary of the then Department of Finance) found that:

---

11 *Constitution* (Cth) s. 51(v).

> Telecommunications interception is a very effective part of an integrated framework of surveillance, it being both cost effective and generally effective.[12]

1.19 Similarly, Victoria Police have reported:

> telecommunications interception is an extremely effective investigative tool, enabling investigators to identify persons involved in, and the infrastructure of organised criminal activities, particularly drug trafficking syndicates. In many cases, the weight of evidence obtained through telecommunication interceptions against a defendant leaves them with no option but to enter a guilty plea, representing significant savings in police resources and court time.[13]

This sentiment was reinforced in the submission of the Victorian Government to this inquiry in relation to electronic surveillance generally.[14]

1.20 The most recent annual report into the operations of the TI Act stated that:

> Evidence obtained from the use of telecommunications interception has resulted in many arrests, the seizure of large quantities of prohibited drugs and criminal assets. Agencies have also commented that the very existence of a telecommunications interception regime serves to frustrate criminal enterprises.[15]

1.21 The significance of TI to law enforcement is demonstrated by the decision of the Commonwealth Government in the May 1999 Budget to provide an additional $8.082 million over four years under the National Illicit Drug Strategy to augment the NCA's and AFP's operational capacity to collect and process evidence obtained through telephone interception. It is noteworthy that surveillance in general is a costly exercise. The NCA has estimated that to run a surveillance team (both electronic and physical) of seven staff for one shift a day costs in excess of $600,000 per annum.[16]

Background

1.22 Prior to the commencement of the *Telephonic Communications Act 1960* there was no statutory prohibition on telephone interception in Australia. The 1960 Act prohibited telephone interception except in very limited circumstances. These included for national security reasons and to enable the Postmaster-General's

---

12 Barrett P.J., *Review of the Long Term Cost Effectiveness of Telecommunications Interception,* Department of Finance, March 1994.

13 *Telecommunications (Interception Act) 1979: Report for the year ending 30 June 1999*, pp. 41-2.

14 *Submissions*, p. 138.

15 *Telecommunications (Interception Act) 1979: Report for the year ending 30 June 2000*, p. 17.

16 NCA submission to Senate Legal and Constitutional References Committee inquiry into the management arrangements and adequacy of funding of the AFP and the NCA, February 2001, p. 27.

Department to trace 'nuisance calls' and for technical purposes. Interception for general law enforcement purposes was not permitted.

1.23 The 1979 TI Act, as originally enacted, enabled interception warrants to be granted only for the investigation of narcotics offences under the *Customs Act 1901*. Since 1987 the offences in relation to which warrants are obtainable have been extended and the number of agencies authorised to apply for interception warrants has increased.[17]

1.24 The broad objective of the TI Act is to balance the need to protect the privacy of communications passing over telecommunications systems within Australia while facilitating appropriate access for national security purposes and by law enforcement. It is designed to protect the privacy of communications passing over a telecommunications system in Australia by:

- prohibiting the interception of communications passing over a telecommunications system in Australia without a warrant; and

- prohibiting the use of material obtained from a lawful or unlawful interception except in tightly defined circumstances set out in the Act.[18]

1.25 The Attorney-General's portfolio submission detailed the essential features of the scheme by which law enforcement agencies are allowed to intercept telecommunications under warrant in accordance with Part VI of the TI Act in the following terms:

- only the AFP, the NCA and certain formally 'declared' State agencies may apply for warrants;

- warrant applications must be supported by an affidavit setting out the information required by the Act to enable the Administrative Appeals Tribunal (AAT) member issuing the warrant to form a view on the matters about which he or she must be satisfied before exercising the discretion to issue a warrant;

- a warrant may be directed at a particular, identified telecommunications service or to any service which a person named on a warrant uses or is likely to use (named person warrants);

- the warrant issuer specifies the duration of the warrant and may impose conditions or restrictions and, in the case of named person warrants, specify particular services which may not be intercepted under the warrant; and

---

17 The 1987 amendments followed a recommendation of Mr Justice Stewart's *Report of the Royal Commission of Inquiry into Alleged Telephone Interceptions*. The Bill was subject to review by a Joint Select Committee on Telecommunications Interception, chaired by S P Martin MP, which reported in November 1986.

18 Attorney-General's portfolio, *Submissions,* p. 213.

- the AFP retains responsibility for overall supervision of all interceptions.[19]

1.26 Part VII of the TI Act makes it clear that telecommunications interception is an act of such significance that its permissible use is restricted in pursuit only of certain serious criminal offences and in certain disciplinary proceedings against AFP officers, State police officers and Commonwealth and State public servants or officers accused of impropriety. These are called class 1 and class 2 offences. Class 1 offences include murder, kidnapping, and narcotics offences. Class 2 offences include offences punishable by imprisonment for life or a period of at least seven years and offences where the offender's conduct involves serious personal injury, drug trafficking or serious fraud.

1.27 As noted at the first dot point in para 1.25, the AFP and the NCA are prescribed in the TI Act as eligible to apply for interception warrants. The Act also provides for 'eligible authorities' to access intercepted information obtained by other intercepting agencies which is relevant to their investigations. 'Eligible authorities' are the police services of each State and the Northern Territory (the Australian Capital Territory being automatically included by virtue of its Agreement with the AFP for the provision of policing services in the Territory), the NSW Crime Commission, the NSW Police Integrity Commission, the Inspector of the Police Integrity Commission, the NSW Independent Commission Against Corruption (ICAC), the Queensland Criminal Justice Commission, the Queensland Crime Commission and the Western Australian Anti-Corruption Commission. The former Royal Commission into the NSW Police Service had also been an 'eligible authority' until its winding up on 26 August 1997. The Police Integrity Commission has assumed many of the Royal Commission's functions.

1.28 Additionally, under section 34 of the Act, if a Ministerial declaration is in force for an 'eligible authority' of a State,[20] then that authority (declared as an 'agency' for the purposes of the Act) can apply for and obtain interception warrants in their own right. As at 30 June 2000 such 'agency' declarations were in force for the Victoria Police, NSW Crime Commission, the NSW Police Service, ICAC, South Australia Police, WA Police Service and the NSW Police Integrity Commission.[21]

1.29 The Queensland Minister for Police and Corrective Services, Hon Tom Barton MLA confirmed in his submission that:

> Queensland legislation does not provide for telephone interception. State investigators can therefore only use telephone interception powers when involved in joint operations with agencies with these powers.[22]

---

19 *Submissions*, p. 213.

20 For the purposes of the Act the expression State includes the Northern Territory (section 5).

21 *Telecommunications (Interception) Act 1979. Report for the year ending 30 June 2000,* p. 5.

22 *Submissions*, p. 91.

This is because section 35 of the TI Act imposes a requirement for there to be in place parallel requirements in State legislation in relation to safeguards and controls on agency access to interception warrants as a precondition to the making of a declaration by the Commonwealth Attorney-General. Thus, all law enforcement agencies which are approved to apply for the issue of interception warrants in their own right operate under equivalent supervisory and accountability provisions, including in relation to inspection and reporting.

1.30 The Attorney-General's portfolio indicates that the TI legislation is designed to be technology-neutral - it applies to any form of communication passing over a telecommunications system whether by voice, fax, images or data. Therefore, it already applies broadly to modern forms of communication which pass over a telecommunications system at some stage, such as the Short Messaging System (SMS), email and other types of Internet communications.[23]

1.31 The final piece of the regulatory picture in relation to TI is contained in the *Telecommunications Act 1997* (Cth). While the principal purpose of the legislation is to regulate the telecommunications industry, Parts 13, 14 and 15 ensure that the industry provides reasonable, necessary assistance for law enforcement purposes. Part 15, in particular, generally requires carriers and carriage service providers to provide, at their expense, an interception capability for each of the services they supply to the public. This facility ensures that a warrant issued under the TI Act can in fact be executed.

Discussion

1.32 The TI Act has been extensively amended since its original enactment, although this process of incremental amendment has been criticised for its tendency to be years behind the telecommunications systems used by criminals for communication.[24] The brief outline of the current state of the legislation given above demonstrates that the particular issue of concern to the former NCA Chairperson, Mr John Broome in 1998 (set out in page xvii of the Preface) in relation to one anachronistic feature of the TI Act, has now been addressed by the Parliament. The passage of the *Telecommunications (Interception) Legislation Amendment Act 2000* (the TI Amendment Act 2000) which in particular introduced the concept of 'named person warrants', has specifically overcome Mr Broome's concern that the legislation was locked into the era of the traditional landline telephone. In its submission to this inquiry, Victoria Police noted:

> The new amendments provide for one warrant to cover all services used by a nominated criminal. A single warrant thus provides access to the multiple SIM and Pre-Paid cards or multiple telecommunications services used by a

23 *Submissions,* p. 213.

24 Confidential submission.

> criminal. This has improved the efficiency with which investigations may be undertaken.[25]

1.33 Previously, the Act had required an agency wishing to intercept all the telecommunications services used by a particular suspect to obtain a separate warrant for each service. The NCA's submission noted that guidelines issued by the Attorney-General's Department had emphasised that a warrant against a person can only be used as a measure of last resort, however.[26] The named person warrant provisions of the TI Amendment Act 2000 will also be subject to review in 2003.

1.34 In his Second Reading Speech in relation to the 2000 Bill the Attorney-General, the Hon Daryl Williams MP, said:

> The amendments … proposed in the Bill will build on and develop the existing legislative scheme to ensure that it continues to support law enforcement and security agencies in the face of developments in technology and the deregulation and globalisation of the telecommunications industry. We must do this if we are to be effective in the fight against crime.[27]

1.35 Evidence to the PJC's inquiry indicates that while the current legislation is a significant advance, especially following the amendments made in 2000, there are suggestions for its further development in view of the increasingly transnational nature of major, contemporary criminality. These include:

- extending the range of offences and assisting foreign investigations;
- extending the purposes for which TI information may be used;
- the Commonwealth devolving some responsibility for TI to the States;
- better regulating the activities of Internet Service Providers; and
- ensuring the currency of the Act's provisions.

The Committee discusses each issue below.

Extending the range of offences and assisting foreign investigations

1.36 The general nature of offences included as class 1 and class 2 offences under the TI Act was detailed in para. 1.26. The NCA submitted that:

> with the expanding use of the Internet and the parallel increase in the scope for Internet effected frauds, there is a case for extending the range of

---

25 *Submissions,* p. 54.

26 *Submissions,* p. 154.

27 House of Representatives, *Hansard,* 16 Feb 00, p. 13491.

> offences for which warrants may be obtained to any fraud offence committed by electronic means ... Other offences that could be considered for inclusion are offences relating to child pornography and stalking.[28]

1.37 The NCA added by way of explanation that the Internet is not simply used to assist the perpetration of offences (which is analogous to the use of a telephone) but is the means by which the offences are committed.

1.38 In the context of a discussion over the lack of arrangements for TI foreign cooperation, representative of the Commonwealth Director of Public Prosecutions, Mr Geoffrey Gray, informed the Committee that the Action Group into Electronic Commerce (AGEC - see footnote 41 for details) had given consideration to having the range of offences widened. He told the Committee:

> The general concept is that if people commit offences electronically then you should be able to go into the electronic medium to investigate them, but the list of offences under the Telecommunications (Interception) Act does not allow you to do that at the moment.[29]

1.39 The TI Amendment Act 2000 introduced the notion of a foreign intelligence warrant, but limited its availability to ASIO only. Mr Gray stressed that 'the fundamental principle [is] that investigative tools which are available to support Australian investigations should be available to support foreign investigations'. He noted, however, that in the law enforcement context there was a 'chicken and egg' problem in relation to TI legislation supporting foreign investigations: it is not clear whether the way forward is to add offences to the TI Act while claiming to support foreign investigations, or whether warrants should be sought for foreign investigations and then look at the offences involved.

1.40 A representative of the Attorney-General's Department, Mr Peter Treyde, added that, because TI is seen as being a highly intrusive investigative technique, the TI Act is framed to impose protective mechanisms on privacy and controls on use of TI information by Australian law enforcement agencies. There remains a concern about how the privacy of Australians can be properly protected when information is passed to foreign law enforcement organisations.[30]

1.41 The Committee appreciates that the current range of offences is prescribed under the TI Act to demonstrate Parliament's recognition that the act of 'tapping' a telephone by law enforcement is a substantial invasion of privacy and should therefore be restricted only to investigations into the most serious of offences. It also acknowledges that there are privacy concerns about the extension of TI powers in support of foreign investigations. However, there is clearly substance to the argument that consideration should be given both to updating the TI Act to accommodate the

---

28 *Submissions*, p. 155.

29 *Evidence*, p. 40.

30 *Evidence*, p. 51.

more serious emerging technological offences and to enable Australia to cooperate with trustworthy overseas law enforcement bodies in pursuit of serious transnational crime.

Recommendation 1: That the Government give consideration to the range of offences prescribed under sections 5(1) and 5D of the *Telecommunications (Interception) Act 1979* in the context of contemporary technological developments.

Recommendation 2: That the Government make TI-related foreign intelligence warrants available to law enforcement agencies.

Extension of purposes for which TI information may be used

1.42 The submission of the NSW Director of Public Prosecutions, Mr Nicholas Cowdery QC, noted that in the May 1997 report of the Royal Commission into the NSW Police Service, Commissioner Justice James Wood had made a number of recommendations for reform of State legislation in relation to electronic surveillance in general (which will be discussed in greater detail in the section below entitled 'Visual and other forms of electronic surveillance') and specifically in relation to TI. Again speaking generally, Mr Cowdery noted that some of the Wood recommendations had since been addressed, while others had not. He wrote:

> For example, despite the recent amendments to extend the use of telephone intercept product in proceedings integrally related to criminal proceedings, such product cannot be admitted in evidence in confiscation proceedings under the Criminal Assets Recovery Act 1990 (NSW) [CARA] (although it can be admitted in proceedings under the Proceeds of Crime Act and its State equivalents, and in Customs Act civil based confiscation litigation). The Wood Report recommended the amendment of the TI Act to allow intercept evidence to be admitted in civil based confiscation proceedings, such as those conducted under CARA (para 7.91).[31]

1.43 Since the publication of Justice Wood's report, the TI Act has been amended on three occasions and amendments made in November 1997[32] were the subject of specific review by the Telecommunications Interception Policy Review, which was completed in May 1999.[33] In its report the Policy Review noted that the 1997 amendments had extended the purposes for which intercepted information could be used in evidence. The report noted comment it had received from the Australian Privacy Charter Council that the amendments had represented an undesirable erosion of the important principle that intercept 'product' should only be used for purposes consistent with the serious crime and national security grounds for which the warrants were granted in the first place.

---

31 *Submissions*, p. 94.

32 *Telecommunications (Interception) and Listening Device Amendment Act 1997.*

33 Attorney-General's Department, *Telecommunications Interception Policy Review,* May 1999.

1.44 The Policy Review did not, however, accede to this call. Rather, it accepted an argument from the NSW Police Integrity Commission that the Act should be amended to enable intercepted communications that had been admitted into evidence in an 'exempt proceeding' to thereafter be admitted in any other proceedings. This recommendation was implemented in the *Telecommunications (Interception) Legislation Amendment Act 2000.*

1.45 A similar argument to that of Mr Cowdery in relation to the exclusion of the *Criminal Assets Recovery Act 1990* (NSW) was made by the NSW Crime Commission but, apart from making mention of the issue, it was not taken further by the Policy Review. Accordingly, the Committee is in no position to conclude whether the TI Act needs further extension as submitted by Mr Cowdery but draws the matter to the Government's attention.

1.46 In the next subsection, the Committee examines calls for the States to be given the right to determine whether the range of offences for which TI is available might be broadened.

The Commonwealth giving devolved responsibility over TI to the States

1.47 Commissioner Wood had made it clear in his report of his concerns about the TI Act, describing it as 'extraordinarily complex and the occasion of real difficulty in application'.[34] The subsequent amendments appear to have met many of the specific concerns raised by the Commissioner in his report. One point of particular concern to him has clearly not been addressed, however. This relates to his call for the:

> devolution of Commonwealth responsibility to the States, at least in relation to the selection of agencies which might use a TI power, and the offences for which it should be available. This is in recognition of the inappropriateness of the Commonwealth being involved in the enforcement of laws at the State level.[35]

1.48 He described the Commonwealth's decision to give the Royal Commission the status only of an 'eligible authority' and not 'agency' status under section 34 of the TI Act (despite the request having been made by the NSW Government, as required by the Act) as 'distinctly unsatisfactory' and a rebuff. He wrote:

> It is difficult to fathom why, in an inquiry involving issues of such profound importance to the people of NSW as the later inquiries revealed [into, for example, paedophile activity] the State should have been denied its wish to confer the full powers it desired on the agency it selected to carry out the

34 Royal Commission into the NSW Police Service, *Final Report,* Volume II, as cited in *Submissions*, p. 96.

35 ibid., p. 99.

> investigation. Certainly the refusal constituted a major restriction upon the Commission's ability to conduct its investigations.[36]

1.49 No submitter to this inquiry pressed this issue directly with the Committee. It caught the Committee's attention because it represented virtually the only issue - if not the only issue - where the Commonwealth rather than the States was being asked to consider giving up some of its constitutional powers in the national interest of future law enforcement coordination and cooperation.

1.50 Given that the NSW Police, NSW Crime Commission, ICAC and the Commission's 'successor', the NSW Police Integrity Commission have 'agency' status, the problem cannot lie with the adequacy of the State's mirror legislation. Rather, it appears that the Royal Commission's rejection by the Attorney-General was based on criteria implicit in the Act for an agency to qualify - that it is a permanent body set up to investigate serious crime, that it is independent and that it is subject to strict accountability requirements.[37]

1.51 This is clearly a complex issue, which probably explains why no submitter chose to raise it with the Committee in the context of such a broadly based inquiry. With the benefit of hindsight of the Royal Commission's achievements, it would not be difficult to sympathise with Commissioner Wood's view that his inquiry deserved a declaration as an intercepting agency because of the significance of the revelations it went on to make. It would also seem to be a fully democratic outcome that, given that the NSW Government had supported the declaration, it alone should be held accountable for the decisions it makes, in the same way that the Government of Queensland is accountable for having chosen the opposite path of not introducing mirror legislation for its own agencies, as noted in para. 1.29.

1.52 The Committee is aware that the NSW Crime Commission also raised similar arguments with the Policy Review, including that it does not seem appropriate that the Commonwealth - which has little constitutional responsibility for the bulk of major crime - should be stipulating the types of crimes for which particular types of surveillance should be used. [38]

1.53 While a delegation to the States in relation to TI would seem to be contrary to the argument underpinning much of this report - that the future of law enforcement in this country in relation to addressing serious inter-jurisdictional crime should be built on more 'national' approaches - the Committee notes that States will still play a critical role in determining their own intra-state law enforcement priorities. Having regard to the long and chequered history of TI (only a portion of which has been able to be

---

36 ibid., p. 100. [Note: While not provided as part of a submission to this inquiry, Commissioner Wood was trenchant in his criticism of the Federal Government's approach to the NSW Government's request for his Commission's direct access to TI in Chapter 1 of Volume 1 of his Final Report, Part K, pages 17-18.]

37 *Telecommunications (Interception) Act 1979: Report for the year ending 30 June 2000*, p. 56.

38 ibid., p. 57.

considered in detail by the Committee), it would be understandable for there to be some sensitivity on the part of the Commonwealth in contemplating giving the States a capacity to broaden the range of offences for which they might use TI information. However, the need for future cooperation between the tiers of Government is an absolute necessity.

1.54 It is also noted that the Commonwealth will be sensitive to Australia's international obligations. For example, Australia has ratified the *International Covenant on Civil and Political Rights* and is a member of the Organisation for Economic Cooperation and Development, both of which place on the Government an expectation to seek to protect privacy from arbitrary interference. Given that surveillance laws such as the TI Act are contrary to principles of privacy, the Commonwealth would undoubtedly wish to ensure that, in order to avoid international condemnation, proper guidelines and safeguards are in place to avoid claims of 'arbitrariness'.

1.55 The Committee recognises that the representations of Commissioner Wood and the NSW Crime Commission are considered and are not made without considerable prior forethought. In the context of comprehensive future discussions about the need for a more cooperative approach to law enforcement, the Committee believes that this issue should be one part of the agenda.

Recommendation 3: That the Commonwealth consult with the Standing Committee of Attorneys-General whether regulation of the use of TI could be delegated to the States and Territories within a continuing context of broad-based mirror legislation.

Better regulating the activities of Internet Service Providers

1.56 The role of Internet Service Providers (ISPs) in their capacity as carriage service providers under the *Telecommunications Act 1997* and, therefore, their obligations under the TI Act, was a matter of considerable discussion by witnesses. As noted above, carriers and carriage service providers have certain obligations under the Telecommunications Act to provide reasonable, necessary assistance for law enforcement purposes. The significance of cooperation between the telecommunications industry and law enforcement is demonstrated by recent statistics from the Australian Communications Authority that some 998,548 disclosures of information (essentially telephone subscriber details) were made in 1999-2000 by carriers, carriage service providers or number database operators in accordance with the provisions of part 13 of the Telecommunications Act. In excess of half of these disclosures were made for the purpose of the enforcement of the criminal law, with some 98% of all disclosures made by the major three carriers of Telstra, Cable & Wireless Optus and Vodafone.[39] The Act also gives the Federal Privacy

39 Senate Environment, Communications, Information Technology and the Arts Legislation Committee, Supplementary Budget Estimates 2000-2001, 30 November 2000, Answer to Question on Notice No. 57.

Commissioner a monitoring role in relation to disclosures of personal information for law enforcement purposes.[40]

1.57 The Action Group into Electronic Commerce (AGEC),[41] which was formed in 1997 by the Heads of Commonwealth Operational Law Enforcement Agencies to research the impact of electronic commerce on law enforcement, identified that one of the key issues in improving law enforcement's response to changing information technology as being 'facilitating appropriate record keeping standards for Internet Service Providers'.[42]

1.58 Several members of AGEC addressed this issue in their individual submissions to this inquiry, while the then Western Australian Minister for Police also raised a range of similar and related concerns. AGEC itself also placed a submission before the Committee to clarify its views, because it felt that there had been some misunderstanding of its position expressed in the Committee's hearings.

1.59 The NCA's submission stated:

> LEAs currently require the co-operation of ISPs to intercept Internet traffic or obtain subscriber details… However, a number of LEA operations indicate that investigators cannot be consistently assured of an ISP's assistance and the low level of regulation (e.g. the absence of formal registration and licensing) raises the risk of compromising an investigation.[43]

The submission went on to note that organised crime figures could establish ISPs, with obviously potential adverse consequences for law enforcement, and that ISPs are not required to retain user information and records that could assist in criminal investigations. Of particular concern to the NCA is the absence of a requirement on ISPs for some form of identity check of their customers.

1.60 In oral evidence the NCA's Mr Irwin stressed that:

> what is important is that the ISPs keep their records for a sufficient period of time to enable law enforcement to gain access to them, just as it gains access to call charge records from the carriers under the Telecommunications Act to indicate who has been talking to whom at what time, so that similar

---

40 In his submission the Privacy Commissioner, Mr Malcolm Crompton, noted that these monitoring powers are in fact quite limited. See *Submissions,* p. 269.

41 The AGEC is chaired by the Director of the Australian Transaction Reports and Analysis Centre, Ms Elizabeth Montano. Its membership includes representatives of the Australian Competition and Consumer Commission, Australian Centre for Policing Research, Australian Federal Police, Attorney-General's Department, Australian Customs Service, Australian Securities and Investments Commission, Australian Taxation Office, Department of Immigration and Multicultural Affairs, Director of Public Prosecutions and the National Crime Authority.

42 *Submissions,* p. 147.

43 *Submissions*, p. 157.

> information is available in relation to those people who are using the Internet to communicate. [Some ISPs cooperate] but at the moment it is entirely voluntary and…while there may be cooperation for law enforcement from the larger Internet service providers the smaller ones do not necessarily cooperate to the same degree.[44]

In making this latter observation, Mr Irwin was endorsing comment contained in the submission of the Australian Bureau of Criminal Intelligence that while the larger ISPs generally keep adequate records, many smaller ones do not, and that consideration should be given to requiring all ISPs to maintain records.[45] He also noted that the keeping of customer records in relation to the Internet was an issue for international attention and that the Council of Europe had proposed appropriate requirements in its draft Convention on Cyber-Crime.

1.61 The submission of the Hon Kevin Prince, the then Western Australian Minister for Police, put forward the view that:

> serious consideration should be given in Australia to placing uniform requirements on ISPs to keep specific logs and other information, relating to the use of their systems, that may be required to identify those involved in criminal activities … Self-regulation and codes of conduct are, with regard to the electronic information industry, insufficient to guard against criminal activities.[46]

The Minister expressed concern that, if ISPs choose to be uncooperative with State police, for criminal or other motives, there may be little that State authorities can do legislatively within their own jurisdictions to seek to enforce that cooperation. This is because of the possibility of Commonwealth legislation being found to take precedence over any State legislation. Given these circumstances, Mr Prince called on the Commonwealth to provide more effective legislation.

1.62 The Australian Securities and Investments Commission (ASIC) also submitted its concerns about the need for better regulation of ISPs.[47] Its submission foreshadowed that the Financial Services Reform Bill - to modernise the regulation of the Australian financial services industry - would also give ASIC some additional enforcement powers to combat computer crime. At the time of preparation of the ASIC submission, it was thought that the Bill would contain provisions to permit ASIC to serve a written notice requiring a person providing services as an ISP to maintain log records created during a specified period of time. It also drew attention to several other proposals expected to be in the Bill, such as a provision to enable it to make mirror images of hard drives of computers during the execution of search warrants and a provision enabling it to serve on an ISP a written notice requiring it to

---

44 *Evidence*, p. 5.

45 *Submissions,* p. 130.

46 *Submissions*, p. 109.

47 *Submissions*, p. 49.

immediately cease providing services where information is placed on the Internet in contravention of the Corporations Law.[48]

1.63 ASIC also offered an additional suggestion for the better regulation of ISPs from a law enforcement, rather than its own corporate regulation, perspective. It suggested that, following the precedent of the *Proceeds of Crime Act 1987,* provision be made for law enforcement to be able to seek a Supreme Court order to require ISPs to monitor transactions through a customer's account.[49]

1.64 The Internet Industry Association (IIA), Electronic Frontiers Australia (EFA) and the Australian Privacy Charter Council responded to these submissions, as did the Federal Privacy Commissioner in relation to the record-keeping and retention requirements for personal information. Ms Mary-Jane Salier provided the IIA's response at a Committee hearing. Ms Salier stressed the IIA's involvement in several governmental committees to assist with the development of regulatory policy and its pioneering role in developing codes of practice for online content regulation in Australia. The IIA had also recently established a Law Enforcement Taskforce, chaired by IIA Director and OzEmail CEO, Mr Justin Milne, to assist its members and law enforcement to address the types of issues being raised with the Committee. The thrust of Ms Salier's evidence was that ISPs are working with law enforcement on the development of appropriate strategies while seeking to ensure that the privacy concerns of their customers are addressed and that no unfair burdens are placed on the industry.

1.65 Ms Salier expressed the industry's concerns about the impact for the industry of the submissions referred to above. In particular she stressed that, in relation to the keeping of records, a distinction had to be made between the notion of records used for billing purposes, which detail when customers log in and log out of their service, and of records of what customers do once online. She placed particular stress on the fact that, unlike call charge records which law enforcement accesses from the major telecommunications carriers, ISPs are not engaged in supplying a point-to-point communications service. They keep no record of 'what sites [customers] visit, what transactions they conduct, what news groups they frequent and what chat sessions they participate in'. They have no need to know this information and such conduct would have privacy and cost implications.[50] She summarised her argument in the following terms:

> I strongly believe that privacy considerations dictate that there should be no general storage of the content of communication and that there should be no general access to the content of communications without the appropriate

48 The *Financial Services Reform Bill 2001* was introduced into the House of Representatives on 5 April 2001. The issues foreshadowed in ASIC's submission were not included in the Bill.

49 *Submissions*, p. 49.

50 *Evidence*, p. 108.

> checks and balances such as those that are currently laid out under the Telecommunications (Interception) Act.[51]

1.66 Electronic Frontiers Australia and the Australian Privacy Charter Council raised similar concerns about requirements for ISPs to keep transaction log records, also from a privacy and human rights perspective. EFA expressed particular concern about a situation where a public authority could gain access to 'a vast wealth of communications data without a ministerial or judicial warrant'[52] while the Council wrote:

> It is one thing to allow law enforcement agencies access, under carefully controlled circumstances and subject to rigorous safeguards, to records already maintained for other purposes. It is quite another to require organisations to effectively spy on behalf of the state - to retain 'intelligence' purely on the basis that it may become useful for law enforcement. To introduce such a requirement would completely upset the balance between privacy and law enforcement in our community and would be a major step down the road towards a surveillance society.[53]

1.67 AGEC subsequently submitted a clear statement of the position taken by law enforcement in these respects. In summary, AGEC stressed that there was no question of seeking records regarding the content of communications, since this was already covered by the provisions of the TI Act. The records being sought are only those which are routinely created by ISPs for billing purposes, which are analogous to the Call Charge Records and Call Associated Data generated by the telephony carriers, and which are governed by the Telecommunications Act. AGEC conceded that there are privacy considerations, but that these are not new considerations and that appropriate provisions and safeguards are largely already in place. The only real point at issue is the length of time that ISPs should be required to retain them.[54]

1.68 The Privacy Commissioner subsequently wrote, in response to AGEC's submission, that there have been calls to subject Call Charge Records to the same access regime as the content of telephone calls:

> The argument is that it is possible to build up a quite detailed picture of a person from traffic data and that where traffic data is used in this way it should be subject to the protection of the [TI Act]. If record-keeping requirements for ISPs carry potential to collate information that is revealing or intrusive then it is likely that higher privacy safeguards will be appropriate.[55]

---

51 Evidence, p. 114.

52 *Submissions,* p. 247.

53 *Submissions,* p. 272.

54 *Submissions,* pp. 254-256.

55 *Submissions,* p. 270.

1.69 There is common ground that storage of records carries costs and, naturally, the larger the ISP and the longer the required period of storage, the greater the cost burden is likely to be. AGEC argued that the cost of storage of records is reasonable when kept in a compressed format on CD ROM or tape. In any case, any costs incurred by ISPs in relation to TI-related requests are paid by law enforcement on a cost-recovery basis.

1.70 AGEC stressed that Australian law enforcement agencies had not yet determined a view on the period for which records should be retained although it was noted that UK agencies had nominated periods of:

- 12 months in a form allowing real-time or live access; and
- a further six years by either the ISP or a Trusted Third Party

in conjunction with proposed ISP record-keeping amendments to the UK's *Regulation of Investigatory Powers Act 2000*.[56]

1.71 The Committee accepts that the same public interest considerations which relate to law enforcement access to records of the telephonic service providers should apply to ISPs. The crux of the issue is that criminals will seek to communicate by whichever form of technology they believe has the least chance of either being intercepted or relevant details being made available to law enforcement. While there may be technical reasons why some services are less capable of being intercepted than others (for example, there is the issue of the capacity of law enforcement to decrypt online communications), and there may be technical constraints to ISPs tracking a customer's multi-point online access, the Committee is concerned to ensure that the legislative regime is not also an avoidable impediment to efficient law enforcement.

1.72 The Committee notes that, while a persuasive case has been made out for better regulation of ISPs, it accepts that it is not well placed to determine the exact details of any such regulation. As the IIA pointed out, the Telecommunications Act is based on the notion of a co-regulatory approach, which seeks to promote the greatest practicable use of industry self-regulation.[57] The international deliberations, discussed in Chapter 3, will obviously also need to be considered in any move to introduce a regulatory regime in Australia. The Committee was also unable to get a full appreciation of the NCA's particular concerns about the absence of both a registration and licensing scheme for ISPs and a requirement on ISPs for some form of identity check of their customers. Both of these issues, as well as that of a possible role for ISPs in assisting law enforcement with decryption, which is a prominent feature of the UK debate, are in the Committee's view matters of some moment.

---

56 *Submissions,* p. 256.

57 *Evidence,* p. 110.

1.73 Accordingly, while the Committee is firmly of the view that ISPs should be better regulated, it urges the parties to continue discussions with a view to finding an acceptable balance between the needs of both law enforcement and the industry.

Recommendation 4: That the Government give particular consideration to the appropriate level of regulation of Internet Service Providers to ensure their cooperation with law enforcement.

Ensuring the currency of the Act's provisions

1.74 While the Attorney-General's portfolio submission made the claim that the TI Act is drafted to be technology-neutral (see para 1.30) and therefore of broad, and seemingly timeless, effect irrespective of mode of communication, it also noted that the transformation of the telecommunications industry arising from the 1997 deregulation has only just begun:

> Further significant developments in the telecommunications market can be expected in the next few years as computer and telecommunications technologies converge. The Government will continue to monitor the legislation closely to ensure it meets law enforcement needs.[58]

1.75 The Committee received additional evidence which emphasised the need for a system of continuous monitoring of technological developments to ensure that the TI legislation keeps pace. The specific issue of greatest concern was the emergence of strong encryption in telecommunications.

1.76 The NCA, for example, submitted that it had encountered a limited number of cases where criminals had used encryption to evade interception. It also noted that, following the Telecommunications Interception Policy Review, there had been established an Inter-Departmental Committee (IDC) on Cryptography, chaired by the Attorney-General's Department and comprising the Defence Signal Directorate, ASIO, AFP, Victoria Police, NSW Police Service, and the National Office for the Information Economy (NOIE).[59] The Committee notes the broad public sector representation on this inter-agency group and urges it to consult with private industry to ensure that its deliberations are realistic and capable of implementation in practice.

1.77 The Wood Royal Commission had included a call for the Government's consideration of 'an effective and workable regime for the continuous monitoring of advances in technology that can prevent their introduction until suitable capacity for intervention is established and that ensures timely and proper amendment of the *Telecommunications (Interception) Act 1979* to meet any such advance and current

58 *Submissions*, p. 214.

59 *Submissions,* p. 157.

needs'.[60] In giving oral evidence, NCA Member Mr Marshall Irwin saw merit in the Royal Commissioner's view:

> It may well be that law enforcement should be given the opportunity to consider those pieces of technology [such as encryption] before they are actually applied and that the people who are providing them are required, before doing so, to make their systems interceptible… by law enforcement agencies.[61]

1.78 The Committee notes that in the *Cybercrime Bill 2001*[62] the Government has proposed that:

> A magistrate would be able to order a person with knowledge of a computer system to provide such information or assistance as is necessary and reasonable to enable the officer to access, copy or print data. Such a power is contained in the draft Council of Europe Convention on Cybercrime and will assist officers in gaining access to encrypted information.[63]

1.79 The Committee believes that it is vital for law enforcement to maintain its capability to intercept and decipher all communications. It calls on the Government to monitor software and hardware developments which, when used in conjunction with telecommunications services, may defeat the purposes of the TI Act.

Recommendation 5: That the Government ensure that the integrity of the TI Act is not undermined by emerging technology.

1.80 Finally in this discussion of TI, the Committee notes that convergence of telecommunications and computing technologies may force the hands of governments in bringing in cooperative legislative solutions. The NCA submission noted one of the ironies of the current Federal system:

> A sent but unopened email needs a TI warrant for interception. Once the email has been downloaded and opened by the recipient it is their property and a search warrant is required. This also applies to Short Message Services (SMS) and voice messages stored in remote locations. These issues complicate the investigative process and may expose covert investigations.[64]

---

60 *Submissions,* p. 95.

61 *Evidence,* p. 19.

62 See Preface, Footnote 13 for details.

63 Hon Daryl Williams MP, Second Reading Speech, House of Representatives *Hansard*, 27.6.01, p. 28641.

64 *Submissions,* p. 156.

1.81 Executive Director of the Australian Information Industry Association, Mr Robert Durie, drew attention to the likely impact of 'wireless' technology:

> wireless is going to be huge, if it is not already, and that is going to lead to ubiquity of access, dispersal, et cetera. If we think that a lot of people are online now and there are a lot of transmissions now, we have not seen anything yet.[65]

1.82 With the General Packet Radio Service (GPRS) wireless data can be delivered to any device whether it be a mobile, Personal Digital Assistant (PDA) or laptop. The information is read and actioned 'live' without copies being made. The Committee simply notes that the 'complications' of the investigative process referred to by the NCA in its submission seem slight when compared to the challenges of the future.

Visual and other forms of aural electronic surveillance

1.83 While physical surveillance of the actions of persons suspected of being engaged in criminal activity will undoubtedly continue to be an important part of the traditional approach to policing, emerging technology over the recent past has permitted law enforcement to substantially expand its capacity to conduct surveillance and, in the process, to collect high quality and compelling evidence against the perpetrators of crime. The NCA submitted that it uses a range of technologies to detect and investigate complex national organised crime:

> For example, investigators utilise electronic surveillance provided by listening devices, miniature video cameras, tracking devices, data capturing devices and telecommunications interception. Investigators also use cyber-forensics to retrieve and analyse data from computers.[66]

1.84 Having examined the telecommunications interception issue above, the Committee will give consideration in this section to the legislative regime which applies to the use of all other electronic surveillance methodologies. It is a substantial and complex topic and is one which has been much studied at both Commonwealth and State level over many years. It could indeed have been the subject of an inquiry by the Committee in its own right. Accordingly, in the interests of succinctness, the Committee will concentrate on the major conceptual issues involved and especially from the National Crime Authority's perspective.

1.85 The types of electronic surveillance discussed below are contentious because they relate particularly to targeted individuals, where the issue of personal privacy is at its most confronting. Governments generally legislate to prohibit use of such surveillance devices, subject to certain exceptions. One of the main exceptions is, of course, in relation to law enforcement where it is argued that the public interest in the investigation and prosecution of criminal activity overrides privacy considerations.

---

65 *Evidence,* p. 84.

66 *Submissions,* p. 146.

1.86 In this context, it is noteworthy that one of the most pervasive surveillance developments in our community appears to have occurred without legislative action. Policing of public places - which has become known colloquially as 'overt' surveillance[67] - has been significantly assisted by the use of enhanced closed circuit television and video technology, with reduced street crime one benefit.[68] The ABCI informed the Committee that offences such as malicious wounding, vehicle theft, robbery and attempted murder have been detected and that numerous offenders have been arrested.[69] The same principle - that there is no general legal rule to prevent the use of a camera to film a person or private property if no trespass is involved - applies also to surveillance of places open to lawful access by the public or places lawfully viewed from a public place.

1.87 Simple video surveillance is now routinely used by shops, commercial premises and workplaces for security reasons[70] and have the added benefit of assisting the detection of criminal offences. There are also clear privacy implications. But, as Justice Wood's report noted: 'law abiding citizens have little to fear from surveillance' and 'those involved in serious crime have no legitimate claim to plan or engage in their criminal activities in privacy'.[71] ABCI commented that it is probable that the community will become increasingly reliant on sophisticated surveillance systems as they go about their daily business in the future.[72]

1.88 The NCA directed its submission to its concerns about the adequacy of Commonwealth legislation and to the 'patchwork' of State and Territory legislation. The Committee draws attention at this point to the overview of the Australian legislative situation given in para. 1.12. The Committee will address each in turn.

Commonwealth legislation

1.89 The *National Crime Authority Act 1984* (NCA Act) is silent on what access the Authority has to surveillance technologies. While the *Australian Federal Police Act 1979*, for example, specifically refers to access to the use of listening devices by AFP personnel in the investigation of a narrow range of offences, the NCA has no such powers clearly declared in its own legislation. Most of its policing powers are in fact those held by its secondees, be they from the AFP or State and Territory police services. Additionally, the AFP submission made the point that:

---

67 See, for example, New South Wales Law Reform Commission Issues Paper 12 entitled *Surveillance*, May 1997, p. 7.

68 The Wood Royal Commission report had noted that in *Bathurst City Council v Saban* (1985) 2 NSWLR 704 it was held that there is no legal prohibition against the use of a video camera in a public place, to film a suspect in a criminal investigation. See *Submissions,* p. 104.

69 *Submissions,* p. 131.

70 Some jurisdictions have specifically legislated to regulate this aspect. Mr Nicholas Cowdery, NSW Director of Public Prosecutions, noted the passage in NSW of the *Workplace Video Surveillance Act 1988.* See *Evidence,* p. 167.

71 See *Submissions,* p. 96.

72 *Submissions,* p. 131.

> Current legislation is not adequate because it is silent on law enforcement use of new technologies. As a result, existing (police) powers and their application in cyberspace are perceived as ambiguous or non-existent… Legislation, therefore, needs to support and ensure the purpose of law enforcement.[73]

1.90 The NCA's powers of federal applicability are declared in general Commonwealth statutes, including in the TI Act and the Customs Act, while its access to powers in State and Territory legislation is subject to provisions in subsection 55A(2) of the NCA Act - only recently inserted by the *National Crime Authority Amendment Act 2000* - which declare that a law of a State may confer on the Authority a duty, function or power that is 'of the same kind' as a duty, function or power conferred on the NCA by Commonwealth legislation.

1.91 The NCA's submission referred to this latter situation as 'unsatisfactory' and went on to state:

> This uncertain test ['same kind'] should be replaced with a provision that clearly permits the use by the NCA of the full range of investigative powers provided by State and Territory legislation which, it is assumed, was the legislative intention. The ideal position would be for those powers to be expressly given to the NCA and its staff members in their own right under the NCA Act.[74]

1.92 It is illustrative of the point that the NCA and AFP submissions seek to make by drawing a comparison between the NCA Act and the legislation underpinning the operations of the Australian Security Intelligence Organisation (ASIO), Australia's principal security intelligence agency. The two organisations have much in common: they both need to operate in a covert manner in the pursuit of their missions and they both need to make use of contemporary surveillance technologies. ASIO differs from the NCA, however, in that it operates within the authority of relevant Commonwealth statutes while the NCA has a dual Commonwealth and State/Territory basis for its power.

1.93 The Parliament made some significant amendments to the *Australian Security Intelligence Act 1979* in November 1999.[75] ASIO subsequently reported that:

> In essence, the changes amount to a modernisation of [ASIO's] current powers to meet the challenges posed by new technology, and to enable ASIO to utilise available technology in the execution of its functions.[76]

---

73 *Submissions,* p. 61.

74 *Submissions,* p. 154.

75 *Australian Security Intelligence Organisation Legislation Amendment Act 1999.*

76 ASIO, *Report to Parliament 1999-2000*, p. 27.

This is, of course, one of the principal interests of the Committee's current inquiry in relation to law enforcement.

1.94 The three main areas of amendment contained in the 1999 ASIO Act as outlined in the Attorney-General's Second Reading Speech were:

- Several provisions to improve ASIO's ability to access information stored in computers. Mr Williams stated that the amendments were necessary given that information relevant to security is frequently stored as computer data. This was not a totally new power. ASIO was already able to examine computer information relevant to security under search warrants and telecommunications interception warrants. The new computer access provisions would allow ASIO to obtain access through other means than were previously permitted.

- A provision permitting the issue of warrants to ASIO authorising the use of tracking devices. The use of tracking devices would permit more efficient use of resources and the amendments were necessary as several State governments were at the time legislating to regulate their use by police and other members of the community.

- Provision was made for ASIO to be authorised to enter property and enter or alter an object for the purpose of installing, using, and maintaining a tracking device. The new provisions were similar to the existing provisions for ASIO's use of listening devices.[77]

1.95 The computer access provisions permit ASIO to gain remote access to a computer from an external computer and, if necessary, to make amendments to data on a computer. The explanatory memorandum stated that this latter aspect included modifying access control and encryption systems. The purpose is essentially to extend ASIO's TI power to emails and, by giving ASIO the ability to access such information via a distant terminal, it is clearly less intrusive and safer for the investigating officer than having to rely on physical search and entry warrant powers. The NCA's submission stated:

> In light of these *ASIO Act* amendments, it may be appropriate for the search warrant provisions in other Commonwealth, State and Territory legislation to be reviewed to ensure that they enable effective searches of computers and other electronic equipment, of the nature provided by the *ASIO Act*. Such provisions, together with closer relations with the [Australian intelligence community], will assist [law enforcement agencies] in circumventing encryption used by criminal syndicates by obtaining direct access to original messages and documents.[78]

77 House of Representatives *Hansard,* 25 March 1999, pp. 4363-64.

78 *Submissions,* p. 156.

1.96 The inclusion of a power to install tracking devices followed a recommendation to that effect in the Walsh report.[79] That report had noted that the absence of this investigative tool was a privation not only for ASIO but also for both the NCA and the AFP.

1.97 The Committee wishes to highlight one other important difference between these ASIO amendments and the NCA situation. ASIO's use of surveillance devices and telecommunications intercepts is subject to audit by the Inspector-General of Intelligence and Security. The Commonwealth Ombudsman, Mr Ron McLeod, has pointed out in his submission that, while his office conducts a specific audit role over the NCA's and AFP's record-keeping in relation to telecommunications intercepts, no similar external accountability arrangements exist for law enforcement's use of listening devices. Mr McLeod's submission stated:

> The question is posed whether the installation and use of listening devices, and the use of video and tracking devices can be regarded as any less intrusive in terms of the invasion of a citizen's right to privacy than a telecommunications intercept. I would support steps to establish more embracive accountability arrangements that would encompass the range of intrusive powers used by law enforcement agencies.[80]

While noting the resource implications for the office of the Commonwealth Ombudsman, the Committee agrees wholeheartedly with the principle that, in the interests of a consistent approach, his office should be given jurisdiction over the use by the NCA (and other relevant law enforcement agencies) of any surveillance device and not simply telecommunications intercepts.

1.98 As will be discussed below, the NCA's access to surveillance devices is largely dependent on State and Territory legislative authority. The Committee accepts the NCA's view that this arrangement is unhelpful and that the situation is best resolved by the inclusion in the NCA Act itself of clear references to the NCA's ability to utilise modern electronic surveillance devices, in a similar manner to that of the ASIO Act. In terms of specific amendments, the NCA pointed to the *Victorian Surveillance Devices Act 1999* as a valuable model.[81]

1.99 Mention should be made of one current development. The NCA's submission had called for the introduction of listening device warrants in respect of the movement of articles in the course of illegal activities by persons unknown at the time of the warrant. Such 'person X' warrants had been considered legal until the decision of the Victorian Court of Appeal in *R v Nicholas.*[82] The Parliament is currently considering

---

79 Walsh, G., *Review of Policy Relating to Encryption Technologies*, 10 October 1996. An edited version of the Walsh Report was released to the Electronic Frontiers Australia (EFA) organisation following a freedom of information application in June 1997 and EFA published it on the Internet at www.efa.org.au.

80 *Submissions,* p. 117.

81 *Submissions,* p. 152.

82 *R v Nicholas* [2000] VSCA 49.

the *Measures to Combat Serious and Organised Crime Bill 2001,* which contains appropriate amendments to the Customs Act that would implement the NCA's recommendation.

State and Territory legislation

1.100 Notwithstanding the problems the NCA experiences from the uncertainty of the 'same kind' provision referred to above, its submission stressed that State and Territory electronic surveillance legislation is a 'patchwork' which impacts adversely on its capacity to coordinate investigations against complex national organised crime, especially when separate warrants need to be obtained in several jurisdictions in the course of the one operation. The 'patchwork' nature of the varying State and Territory legislative provisions in relation to electronic surveillance was described in the following terms:

> The legislation in Victoria, Western Australia and Queensland provides for the use of a wide range of surveillance devices. [Footnote in orginal: The Victorian *Surveillance Devices Act 1999* refers to data surveillance devices, listening devices, optical surveillance devices and tracking devices. The Western Australia *Surveillance Devices Act 1998* refers to listening devices, optical surveillance devices and tracking devices but not to data surveillance devices. The Queensland PPR Act (*Police Powers and Responsibilities Act 2000*) refers to listening devices, visual surveillance devices and tracking device or any combination of those devices.] The legislation in New South Wales provides for composite listening/video and listening/tracking devices. Legislation in other jurisdictions is confined to the use of listening devices.[83]

1.101 The patchwork status of legislation raises the issue of the application of cross-border operations where what might be authorised in one State may not be similarly permitted in another. The NCA submission noted:

> For example, a listening device may be installed in a vehicle travelling across state and territory jurisdictional boundaries. Successful surveillance requires different and separate warrants to be obtained for each jurisdiction. This is a particular problem for the NCA investigations that have a national and international focus.[84]

1.102 Victoria Police's Detective Inspector Stephen Berriman echoed the NCA's concerns when he described the practical implications for the Victoria Police in relation to tracking a drug courier from Victoria to New South Wales:

> At this stage, we would take out a warrant in Victoria under the Surveillance Devices Act for a tracking device… Once it hits the border, it goes into New South Wales. The New South Wales legislation is silent on the use of

83 *Submissions,* p. 153.

84 ibid.

> tracking devices at this time, so there is no prohibition … We can still track it.[85]

However, if New South Wales were to introduce tracking devices legislation, Victoria Police would commit a criminal offence if it did not obtain an appropriate NSW warrant.

1.103 Both the NSW Director of Public Prosecutions, Mr Nicholas Cowdery QC, and Detective Inspector Berriman noted that, if a surveillance device operating pursuant to a warrant within one State travels out of the State, there could subsequently be evidentiary problems when the matter comes to court.[86]

1.104 Detective Inspector Berriman also explained to the Committee that the impediment to installing tracking devices at the federal level is the issue of 'trespass re-entry'. He said:

> There is legislative support to actually place a device on a vehicle or on an object, and for the entry to premises to retrieve it - and it may not be the same premises. Once you have placed these devices, particularly in a mobile environment, you have to have contingency plans to retrieve [them] … That is not possible without legislative support.[87]

The NCA's submission clarified that, while Victorian legislation might authorise the trespass where necessary to install a tracking device and a data surveillance device, no State other than Victoria permits data surveillance and the different States have differing provisions in relation to tracking devices. It stressed the 'important need' for all jurisdictions to enact legislation to authorise the 'trespass'.[88]

1.105 In his submission, Commissioner of the Northern Territory Police, Mr Brian Bates, made this general comment:

> It is recognised that there are current inadequacies within the Commonwealth, State and Territory legislative frameworks to cater for technological changes … policing needs to respond to technology in a coordinated and consistent manner to address crimes that will routinely cross domestic and international jurisdictions.[89]

1.106 The Committee has been down this path before. In its December 1999 report *Street Legal: The Involvement of the National Crime Authority in Controlled Operations* the Committee recommended that the Commonwealth, States and Territories should seek to introduce uniform controlled operations legislation. While

---

85 *Evidence,* p. 129.

86 *Evidence,* pp. 167, 130.

87 *Evidence,* p. 129.

88 *Submissions,* p. 154.

89 *Submissions,* p. 45.

the Commonwealth Government indicated its agreement to this recommendation, it saw the quest for uniformity as a 'medium term' goal while it agreed to press ahead with pursuing the enhancement of Commonwealth provisions in the first instance.[90]

1.107 This approach, while understandable, still suggests a regime of disparate legislation across jurisdictions for the foreseeable future, with criminals (and lawyers) the main beneficiaries. The ideal situation from a national perspective is national legislation. Australia also has been down this path before. The introduction of *The Corporations Law* in 1989 was one of the more prominent examples of national cooperation to overcome a national regulatory problem, despite the subject matter being constitutionally a State matter. Another was the introduction in 1996 of a National Classification Code for the classification of publications, films and computer games, although States retained the enforcement role in that case. Even as far back as the 1930s the States cooperated with the Commonwealth on the issue of the regulation of intrastate aviation, which system of regulation was patently contradictory to the national and international nature of the industry.

1.108 The Committee recognises that the States and Territories may wish to take a different view about the merits of national legislation in relation to the use of surveillance devices and computer-attack capabilities within their jurisdictions. In the submission of the then Australian Capital Territory Attorney-General (and now Chief Minister), Mr Gary Humphries MLA, he noted two areas where the ACT has no legislation in relation to law enforcement access to computer-based information, noting 'these matters have yet to be considered by the wider legal community in the ACT'.[91] As stated earlier, Queensland has introduced comprehensive surveillance devices legislation but has still not decided to introduce telephone interception legislation, even after some 20 years of practical experience elsewhere. Yet in 1998-99 the Queensland Police made seven arrests on the basis of intercepted information obtained under warrant by either the NSW or Victoria Police.[92]

1.109 The NSW Director of Public Prosecutions, Mr Nicholas Cowdery, stressed his view that legislation in NSW had lagged behind developments in the technology available to law enforcement agencies. He drew attention to the recommendation of the NSW Drug Summit 1999 that the law relating to electronic surveillance, listening devices, search warrants and controlled operations should be urgently enhanced to assist police in quickly targeting drug traffickers.[93] Mr Cowdery also noted that the NSW Law Reform Commission had commenced an inquiry into the law relating to electronic surveillance in July 1996, had issued an Issues Paper in May 1997 entitled *Surveillance* and had finalised its interim report in February 2001. At the time of writing, this interim report had not been published. Finally, Mr Cowdery highlighted

---

90 Senate, *Hansard,* 29 March 2001, p. 23361. See Measures to Combat Serious and Organised Crime Bill 2001 for details of the Government's initiatives in this respect.

91 *Submissions,* p. 65.

92 *Telecommunications (Interception) Act 1979*: *Report for the year ending 30 June 1999,* p. 42.

93 NSW Drug Summit 1999, *Communique*, 21 May 1999, para 9.15.

the recommendations of the Wood Royal Commission on the need for the State's *Listening Devices Act 1984* to be updated. Some of the problems identified have been resolved in more recent amendments, while others remain.[94]

1.110 In general terms, the current patchwork of State and Territory legislation speaks for itself. This level of variation at the State and Territory level does not bode well for agreement on national legislation in the short term, although the Committee was heartened by the advice of Mr Karl Alderson, a senior officer of the Attorney-General's Department, that under the auspices of the relevant Ministerial councils there is a dedicated group of Commonwealth and State experts on uniformity and consistency of law enforcement legislation.[95] As the Government stated in reference to uniform controlled operations legislation, progress is more likely to be a medium term goal.

1.111 However, there is one possibility which could prompt this matter to gain momentum: the development of an international convention which, should Australia become a signatory, might provide the Commonwealth with constitutional authority under its 'external affairs' power to introduce national legislation which would override State and Territory legislation to the extent of any conflict or inconsistency. As detailed in Chapter 3, much work on cross-jurisdictional computer-based crime is being undertaken, such as that of the Council of Europe Draft Convention on Cyber-Crime. And, as pointed out by the Federal Privacy Commissioner, a small country like Australia may find itself having to be a policy taker in areas which may not always or in all respects fit well with our legal system or structure, given the adverse consequences which might flow from non-cooperation.[96]

1.112 The Committee notes that, with such awareness of the need for the standardisation of laws at the international level, it can only be a matter of time before Australia will have to commit itself to a similarly cooperative scheme at the national level.

1.113 In the absence of agreed national legislation the NCA, Victoria Police and Mr Cowdery suggested that the issue can best be dealt with by the making of uniform amendments to the respective State and Territory surveillance devices legislation to provide for extraterritorial operation and mutual recognition.[97] The use of technology neutral language, which will incorporate all existing and foreseeable devices, is also seen as desirable. Thus, under a fully national cooperative scheme, any warrant issued in one jurisdiction for anything of a surveillance devices nature would not only be declared as having effect across State borders at the time of its issue, but would also be granted validity within the law of the 'receiving' State. Recent amendments in

---

94 *Evidence,* p. 166, and *Submissions,* pp. 93-94.

95 *Evidence,* p. 45.

96 *Submissions,* p. 260.

97 *Submissions,* pp. 153-54, and *Evidence,* pp. 130, 166.

section 195 of the Queensland *Police Powers and Responsibilities Act 2000* are seen as providing a model in this respect. This process has been depicted as one of 'harmonisation' of the disparate State and Territory legislative regimes, which is an apt description given its current discordant state.

1.114 The NCA noted with approval the introduction in the United Kingdom of the *Regulation of Investigatory Powers Act 2000* as a model for Australia. That Act contains provisions that go beyond the types of investigatory powers currently accepted as the norm in legislation in Australia and its introduction in the UK has not been without considerable controversy. However, it is more the manner in which the Act codifies relevant laws for the whole country that the NCA has sought to endorse. In terms of certainty of the operations of the law, it would seem sensible to add (or, indeed, delete) investigatory powers within the framework of a single piece of legislation, rather than having them scattered throughout the statute books.

1.115 The UK Act is designed to ensure that the relevant investigatory powers are used in accordance with human rights. It encompasses the interception of communications, intrusive and covert surveillance, the use of covert human intelligence sources (such as agents, informants and undercover officers), the acquisition of communications data; and access to encrypted data. Importantly, for each of these powers, the law clearly states the purposes for which they may be used; which authorities can use the powers; who should authorise each use of the power; the use that can be made of the material gained; independent judicial oversight; and a means of redress for the individual.

1.116 In the Australian situation, emphasis would need to be placed on the types of provisions currently contained in the *Telecommunications (Interception) Act 1979* such as the need for judicial supervision of the investigatory processes, uniform oversight of the adequacy of all administrative processes by the relevant Ombudsman,[98] and high standards of accountability through reporting to the Minister and the Parliament.

Recommendation 6: That, in conjunction with the States, the Government introduce comprehensive national electronic surveillance legislation, with particular emphasis on the inclusion of appropriate privacy provisions.

Information and intelligence systems

1.117 While information technology (IT) is playing an ever-increasing role in criminal activity - with traditional crimes such as fraud and the exchange of child pornography now performed in an online as well as the offline environment - the efficiency of law enforcement has also been significantly assisted by IT developments. Agencies such as the NCA gain considerable benefit from the use of current technologies in the management and storage of information and intelligence systems. The NCA's submission detailed a case study of an investigation into large-scale tax

98 The Commonwealth Ombudsman currently oversights the use of TI by the NCA and the AFP.

evasion where large amounts of documentary evidence and IT evidence gathered from the hard drives of seized computers was able to be analysed by use of sophisticated computer applications.[99]

1.118 The benefits of such modern IT developments to any one law enforcement agency tend to be limited more by budgets than by the quality of legislative support to their use by governments, which is the Committee's principal interest. However, one of the more important aspects of IT in law enforcement is the manner and extent to which agencies are able (and willing) to exchange their valuable intelligence material with each other. While bilateral, agency-to-agency transfers of information would occur regularly under Memorandums of Understanding, the development of multilateral exchange has required the active involvement of the several Australian governments. This process has led in particular to the establishment of two agencies: the Australian Bureau of Criminal Intelligence (ABCI) and the CrimTrac Agency.

1.119 The ABCI was established in 1981 to improve intelligence cooperation and coordination between Australian police services. At that time it dealt with just eight police services - it now has in excess of 38 agencies with which it exchanges law enforcement information. It is non-operational and relies on client agencies for the collection of information in the field. Funding of the ABCI reflects its national character. Being established as one of the national common police services under the jurisdiction of the Australasian Police Ministers' Council, it is not a Commonwealth agency but it nonetheless receives the bulk of its funding from the Commonwealth Government, as well as supplementation from State government sources.

1.120 To achieve its goals it provides a range of IT services, training programs and analytical assistance to its client agencies. Access to ABCI information is through the Australian Law Enforcement Intelligence Net (ALEIN). ALEIN is a secure, national extranet used by all Australian police services and a large number of government law enforcement agencies. It is a universal system that fosters the sharing of criminal intelligence, especially as its use is not dependent on the type of hardware in use by the client agency. Through web browser technology, ALEIN acts as a gateway to the ABCI's document-based reference material and structured databases such as the Australian Criminal Intelligence Database (ACID) and the Violent Crime Linkage Analysis System.

1.121 The ABCI acts as a custodian of the information placed on its systems by law enforcement agencies. Importantly, given that management of criminal intelligence is an important issue for all law enforcement agencies, the client agencies retain ownership and control of their data.[100]

---

99 *Submissions,* p. 158.

100 *Submissions,* p. 136.

1.122 The NCA uses ACID and ALEIN as the repositories of intelligence for the task forces it coordinates under the NCA Act[101] but its submission to this inquiry emphasised that its capacity to disseminate information to some agencies was uncertain because of doubts about whether they are 'law enforcement agencies' for the purposes of the NCA Act. This is taken to be a reference to section 59 of the NCA Act. Regrettably, while the Government has proposed amendments in the *National Crime Authority Legislation Amendment Bill 2000 [2001]*, which was before the Parliament at the time of compilation of this report, to amend section 59 to enable the NCA's Chairperson to disseminate information to foreign law enforcement agencies, it failed to define with greater clarity to which domestic law enforcement agencies the NCA Chairperson can provide information. The Committee draws this matter to the Government's attention.

1.123 The ABCI noted, and the submission from Canberra-based software company, The Distillery Pty Ltd confirmed,[102] that information cooperation is far from perfect because law enforcement is subject to restrictions on the use to which it can be put. The ABCI submitted:

> Privacy, Freedom of Information, Call Charge Records (CCR), telephone interception (TI) information and the requirement to restrict data collected by use of coercive powers is placing such a legislative and resource burden on agencies that they are often unwilling or unable to put information into databases such as ACID. In cases where agencies do include intelligence which might be tainted with CCR or TI information, it is usually caveated to such a degree that it is unavailable to other law enforcement officers around Australia.[103]

1.124 The Committee recognises that some constraints on the use to which law enforcement information can be put are desirable, but it also notes that for databases to be effective, maximum cooperation is desirable.

Recommendation 7: That the Australian Government place on the agenda of the Standing Committee of Attorneys-General the need for a comprehensive and fundamental review of the operations of legislative provisions that may inadvertently and unnecessarily restrict the capacity of law enforcement to exchange intelligence and operational information.

1.125 CrimTrac has evolved out of another of the national common police services, the National Exchange of Police Information (NEPI). The announcement of CrimTrac's intended establishment was made by the Prime Minister in October 1998 and in the 1999 Budget some $50 million was committed for its first three years of operation. CrimTrac is a new national crime investigation system which, by using

---

101 NCA, *Annual Report 1999-2000,* pp. 18-19.

102 *Submissions,* p. 81.

103 *Submissions,* p. 133.

state of the art technology, will provide Australia's police with real time access to some of the information they need to make the task of solving crimes more efficient and timely. CrimTrac will include:

- an enhanced National Automated Fingerprint Identification System (NAFIS);
- a new national DNA database; and
- a national Child Sex Offender register, for police use only.

CrimTrac will also provide Australia's police with fast access to operational information including domestic violence orders, person warnings and stolen vehicle information.

1.126 The CrimTrac Agency was established as an Executive Agency under the Commonwealth *Public Service Act 1999* on 1 July 2000 and operates under an intergovernmental agreement signed by all police ministers. Its predecessor - NEPI - now no longer exists. The Agency's work will complement that of the ABCI. While ABCI represents a central intelligence resource, CrimTrac will deliver advanced operational information services and investigation tools to the nation's police. With increasing human mobility between States and Territories, the need for national databases is clear. Importantly, CrimTrac has the formal support of all State and Territory Governments, which will be responsible for contributing to the cost of its administration in the long term.

1.127 NAFIS was first established in 1986 and became one of NEPI's main functions when it was created in May 1990.[104] At that time NAFIS was a world leader in allowing operational officers to match fingerprints held on a central National Database. However, after 13 years of operation, its technology had been overtaken in countries such as Europe, the United States and New Zealand. It was also a relatively slow process. The fingerprinting process involving printers ink, a roller and a slab had barely changed throughout its century of operations. The prints - whether obtained at the station or from the crime scene - had to be posted to NAFIS where they were scanned and searched against the 2.3 million records held in the database. A fingerprint expert then had to verify the match. The poor quality of the prints often thwarted a match.

1.128 CrimTrac's new fingerprint system will make use of the latest livescan technology. Livescan's inkless process uses electronic and laser technology to scan fingers and palm from a flat glass pad to produce a clear and undistorted record. Police officers can then feed the electronic fingerprints to CrimTrac for an immediate search. If they are holding a suspect in custody, such speedy responses will be invaluable.

---

104 Specific details of CrimTrac's operations have been sourced from CrimTrac Factsheets issued by the Attorney-General's Department. See also *Submissions,* pp. 237-240.

1.129 The National DNA Database will similarly revolutionise crime investigation. Australian police have largely relied on DNA evidence in seeking to solve individual cases, by matching DNA taken from a particular suspect to DNA evidence recovered from a crime scene. Two States and the Northern Territory had established their own local DNA databases, which were effective but jurisdictionally limited. DNA evidence has been used to convict persons of offences such as sexual assault, armed robbery and murder, but it has also established the innocence of many others implicated in a crime. The recent mass screening of volunteers in Wee Waa, for example, helped eliminate suspects in a criminal investigation as well as, ultimately, contributing indirectly to a conviction.

1.130 CrimTrac's National DNA Database will contain DNA profiles of existing convicted serious offenders which can be matched against samples obtained from suspects or crime scenes. Because a large number of crimes are committed by a small number of criminals, once criminals have their DNA profile recorded on the database, police will be able to identify them faster. CrimTrac is expected to hold about 25,000 DNA profiles in its first year, with more being added continuously.[105]

1.131 Collection and matching of DNA profiles will be undertaken in accordance with legislation. At the time of writing, the Commonwealth and all States and Territories except Western Australia had passed the necessary legislation to establish the database and to permit DNA samples to be taken from convicted criminals.[106] Despite the legislation having been developed by the Model Criminal Code Officers Committee with the Hon Judge R N Howie QC as its chair, and with input from representatives of all jurisdictions, Mr Cowdery made it clear that the legislation 'struck all the barriers that we are accustomed to between jurisdictions, and it is very frustrating'.[107]

1.132 The world's first national criminal DNA database was established in the United Kingdom in April 1995 and by 1999 held over 500,000 DNA records. Over 10,000 matches had been made between crime scenes and suspects and on average 333 crimes were cleared up per month.[108] More comparable to the Australian federal situation, the United States Federal Bureau of Investigation created a national DNA database in 1998, enabling police to solve multi-jurisdictional crimes, such as of serial rape or murder, where the perpetrator may have moved between states.

1.133 Witnesses to this inquiry from law enforcement, not surprisingly, lauded the development of CrimTrac as a major technological advance in the fight against crime. Emphasis was placed by Dr John Gaudin of Privacy NSW, however, of the need for

---

105 AAP, *Launch of CrimTrac means old cases can be re-examined,* 20 June 2001.

106 The Commonwealth *Crimes Amendment (Forensic Procedures) Act 2001,* Act No. 22, 2001, received assent on 6 April 2001.

107 *Evidence,* p. 170.

108 Report of the Model Criminal Code Officers Committee, *Model Forensic Procedures Bill and the Proposed National DNA Database,* May 1999, p. 1.

high standards of accountability for such database operations in view of their capacity for broad, proactive policing rather than the traditional and more specific investigation of particular offences, which are supervised by judicial officers through warrants and courts exercising their discretion to exclude improperly obtained evidence.[109]

1.134 In its submission, the Victorian Government stressed that its amendments to its *Crimes Act 1958* had, through judicial supervision, ensured an appropriate balance between individual rights and a technology which is regarded by experts worldwide as the most important scientific advance to be offered to the criminal justice system since the development of fingerprint analysis.[110] While Mr Cowdery noted the civil liberties argument that the compulsory acquisition of a person's DNA record is a breach of human rights, he noted that it could be justified by reference to the limited use to which the DNA information could be put - to assist in resolving criminal offending - and that the safeguards contained in the national model legislation assure that the right balance has been struck.[111]

1.135 The Committee strongly endorses the operations of such national databases as a positive means of breaking down the jurisdictional barriers. Not only should Australia seek to remove the protection such jurisdictional barriers provide to criminals, civil liberties are enhanced where such processes confirm innocence as well as guilt. The Committee endorses this comment in the MCCOC report:

> Justice is about getting to the truth, anything that helps in that process should enhance the quality of our justice system.[112]

Laws of evidence

1.136 Several submitters noted that the operations of State and Territory Evidence Acts are also affected by new technology, with the Queensland Minister for Police and Corrective Services in particular pointing to inconsistencies between Commonwealth, State and Territory legislation relating to the preservation of evidence.[113] It would, of course, be a matter of considerable concern to law enforcement if any evidence that had been obtained by use of emerging technology was not accepted as admissible in the courts. As noted above, both Mr Cowdery and Detective Inspector Berriman noted that evidentiary problems may arise when a surveillance device issued under warrant in one jurisdiction moves out of that jurisdiction.[114]

---

109 *Evidence,* p. 134.

110 *Submissions,* p. 139.

111 *Evidence,* p. 173.

112 Report of the Model Criminal Code Officers Committee, *Model Forensic Procedures Bill and the Proposed National DNA Database,* May 1999, p. 4.

113 *Submissions,* p. 91.

114 *Evidence,* pp. 130, 167.

1.137 A representative of ASIC, Mr Keith Inman, informed the Committee that even though ASIC officers operate under a national scheme, they have to take account of the different evidence rules which apply in the jurisdiction in which they are operating.[115]

1.138 The two submissions to this inquiry from Tasmanian Government sources both alluded to the admissibility issue, particularly in relation to photographic evidence obtained by digital imaging and especially for remote devices where there is no evidence from a person who took the photograph.[116]

1.139 NCA witnesses noted that the issue of digital cameras is significant and that there is a fear that electronic data may be more capable of being manipulated than when evidence is in conventional form. They made the point that, at present, courts seem to be willing to accept electronic material in the same way they have traditionally accepted documentary evidence, provided it is properly authenticated.[117]

1.140 In relation to electronic crime, the Attorney-General's portfolio submission noted that:

> The CDPP (Commonwealth Director of Public Prosecutions) can only prosecute cases which involve e-crime if the investigators have the tools they need to properly investigate the alleged offences, collect the evidence needed to prove them and be able to present the evidence in court. This presents a challenge which, while formidable, can be addressed provided that the criminal law, the laws of investigation and the rules of evidence are all kept up to date and are not allowed to lag behind the changing nature of criminal activity.[118]

1.141 The then Western Australian Minister for Police advised the Committee in his submission that admissibility of copies of information obtained under analysis had specifically been one of the issues addressed in a draft Bill prepared in 1999 to tackle computer-based crime in Western Australia.[119]

1.142 In a related matter, the NCA drew attention to the requirement to vary the form and manner in which particularly electronic evidence is presented in court to comply with the laws and procedures of each jurisdiction, while also noting that several jurisdictions have examined their laws of evidence and procedures to permit the greater use of computer facilities in courts.[120] The Committee was advised by the Australian Institute of Judicial Administration of the conduct in October 2000 of a

---

115 *Evidence,* p. 162.

116 *Submissions,* pp. 42-43.

117 *Evidence,* pp. 21-22.

118 *Submissions,* p. 198.

119 *Submissions,* p. 108.

120 *Submissions,* p. 159.

conference entitled 'Technology for Justice 2000' where the use of information technology in support of the administration of justice was discussed. In July 2001 Queensland's University of Technology launched the first purpose-built e-courtroom to help teach law students. Temporary e-courts have hosted cases in the Federal Court and in the Supreme Courts in NSW, Victoria and Western Australia.[121]

1.143 It is clearly only a matter of time before real e-courts are established, as they have been in the United States and Singapore. The Committee notes efforts internationally through the International Organisation of Computer Evidence to establish 'common' computer evidence standards to combat criminal activity that has crossed international borders.[122]

1.144 It again encourages Australian governments to work cooperatively to introduce modernised and harmonised requirements in relation to the admissibility of evidence in the interests of advancing the administration of justice within Australia.

Accountability

1.145 In appropriate contexts elsewhere in this Chapter the Committee has addressed the need for caution in giving law enforcement unfettered access to all the latest technological developments. Some Committee members were troubled by the overall implications for society of the aggregated outcome of the extent and range of intrusive surveillance and database operations of the types discussed, especially when the transition from the physical world to cyberspace is taken into account.

1.146 The issue of the use to which law enforcement might put the ever larger volumes of material it could access in the future was addressed directly by NCA representatives, Marshall Irwin, and Mr Adrien Whiddett, the NCA's General Manager Operations. Mr Irwin noted:

> We appreciate that that is … a live issue and…there is a balance to be drawn… Mechanisms could be built into the process such as already exist in telecommunications interception legislation, for example, and a range of other electronic surveillance legislation, where the intrusion can only occur through the authorisation of a judge or a sufficiently qualified judicial person, and that there be some external overview of the way in which the Authority or any other agency discharges those functions, for example, by extending the role of the Ombudsman or someone similar. I would accept…that any additional powers that agencies were given in this regard would have to be balanced by those types of accountability mechanisms. Obviously, if there were to be judicial approval or a judicial warrant, there would be strict legislative criteria that would have to be complied with before the warrant could be obtained.[123]

---

121 AAP, *Australia's first purpose-built e-court opens,* 4 July 2001.

122 Comprehensive details in *Submissions,* p. 231.

123 *Evidence,* p. 7.

Mr Whiddett added:

> The same [concept] applies for listening devices and telephone interception; in other words, the warrants have been taken out for a good reason and provided by a judge…in the midst of a lot of dross there may only be a few pearls of something interesting. That is the reality at present. There would be a vast amount of material gained by that means, which has no particular interest to the matter in hand but may be of a general nature. It is a question of discerning what is valuable to law enforcement and what is not.[124]

1.147 By way of clarification, Mr Irwin stressed that:

> law enforcement does not have any interest in that sort of information [private and personal] and does not have any interest in trading in that sort of information. It is clearly only interested in that information that advances its investigations in the discharge of its functions.[125]

He added that investigatory material is accorded a high classification at the NCA and that it is breach of the NCA Act for an officer to disclose it other than for the purposes of the Act.

1.148 The AFP submission similarly stressed:

> If the law gives agencies the power to intercept communications, then that power should apply to whatever may in future be considered communications. If legislation is tied to specific technologies, then legislation will have to be rewritten whenever technology advances. The problems being faced now will simply recur.[126]

1.149 The NCA pointed to the existing role of the Commonwealth Ombudsman in oversighting NCA and AFP use of telecommunications interception and the fact that the Ombudman's office had only ever reported a high level of conformance with the provisions of the TI Act, apart from 'minor clerical errors'. This was confirmed by Senior Assistant Ombudsman, Mr Philip Moss:

> …our experience has been that any errors or problems identified during those inspections are quickly addressed and corrected by the law enforcement agencies. As a consequence, our inspections have been instrumental in bringing about changes to the processes that assist in maintaining compliance with the requirements of the TI Act.[127]

1.150 The main thrust of the Ombudsman's submission, as described in para 1.96, was that the current accountability regime is inconsistent. As Mr Moss put it:

---

124 *Evidence,* p. 8.

125 *Evidence,* p. 9.

126 *Submissions,* p. 61.

127 *Evidence,* p. 86.

> The information obtained through a listening device may have a similar content or value to that obtained though telecommunications interception, yet the user of the device is not subject to similar oversight inspection.[128]

The Committee strongly endorses the concept of a consistent accountability regime. It is also important that there is a sound system of independent review of the activities of law enforcement in relation to all use of intrusive measures. Such independent review would provide assurance to the Minister, the Parliament and the public that law enforcement agencies are complying with legislative safeguards with integrity (it is worth noting that the courts will also deal with any illegalities) and respecting citizen's rights.

1.151 In relation specifically to privacy, the NCA submitted that, at all times in carrying out investigations, it is sensitive to privacy implications. Although exempted from the provisions of the *Privacy Act 1988* the NCA seeks to ensure that the collection, use and storage of information is subject to appropriate controls and safeguards. [129] In his submission the Federal Privacy Commissioner, Mr Malcolm Crompton, stressed the importance of privacy to the Australian community but also recognised that finding the right balance between privacy and effective law enforcement does involve complex and difficult judgements. He submitted:

> In looking at future directions in crime prevention including legal and policy responses it is important to recognise that our individual privacy is often taken for granted. Privacy is clearly perceived by Australians as a fundamental human right, and a right we are eager to preserve in a rapidly changing global environment.[130]

1.152 Mr Crompton noted that the impact of crime prevention measures or additional investigative powers will range along a spectrum of privacy intrusiveness and he suggested that the following matters should be considered before additional investigative powers are implemented and granted:

- the power should be conferred, or the measure introduced, expressly, not by implication;
- privacy intrusive powers or measures should be conferred by an Act, not by subordinate legislation;
- the grounds on which power of intrusion may be exercised should be stated expressly and in objective terms;
- the authority to exercise intrusive powers, for example search or seizure should generally be dependent on special judicial authorisation (a warrant); and

---

128 *Evidence,* p. 86.

129 *Submissions,* p. 149.

130 *Submissions,* p. 259.

- other intrusive activities, for example seeking documents using statutory notices or other legislative mechanism, would at least require an appropriately senior officer to authorise the activity.[131]

The Committee strongly endorses these considerations.

1.153 Legal and Policy Officer for Privacy New South Wales, Dr John Gaudin, told the Committee:

> Accountability for the use of intrusive powers requires a greater openness than has often been the case. Law enforcement agencies often argue that people should be prepared to trust their high security and confidentiality standards rather than expect specific measures to deliver accountability. My response is that we cannot assume that powers will not be misused. This is not necessarily restricted to conscious corruption… It can also include overzealousness and impatience with playing by overly formal rules, or the effect of a cultural attitude in law enforcement based on the sense of knowing so much more about the people you are dealing with that you have had the sense of superiority to them.[132]

1.154 Dr Gaudin emphasised that Privacy NSW is concerned about escalating surveillance and, in recognition of the established tradition of judicial warrants to approve intrusive searches, it would wish to see the concept broadened to encompass a 'clear privacy framework' with 'clear legislative safeguards' as new forms of surveillance are approved. He pointed to the absence of any warrant provision over police access to traffic data under the Telecommunications Act as one specific omission in the safeguards structure.

1.155 The Committee notes that the general community appears to have come to accept surveillance as a fact of life, especially as a means of preventing crime. It is in use in the streets, in the shops, in workplaces, in sports stadiums and in casinos. The Wood Royal Commission noted in its report that a March 1997 Morgan-Bulletin Poll had found that 89% of respondents approved of the use of surveillance cameras in public places and 57% in the workplace.[133]

1.156 Similarly, the Federal Privacy Commissioner noted that his Office's research had shown that 57% of respondents would be happy for police to have more access to information on databases if it led to a significant increase in crime prevention. He stressed, however, that the raw data did not adequately reflect people's lack of knowledge and understanding of privacy, and that they may hold different views if they were more aware of how personal information is handled, including for law enforcement purposes. He pointed out that the community probably does have limits to the amount of invasion of privacy it is prepared to bear, such as resisting global

---

131 *Submissions,* p. 267.

132 *Evidence,* p. 134.

133 In *Submissions,* p. 96.

DNA or fingerprinting of whole populations, with its attendant suggestion that we are guilty until proven innocent.[134] As a practical example of such concerns, all samples other than those of the accused were destroyed some five months after the mass DNA sampling undertaken in Wee Waa was completed.[135]

1.157 As the AIIA pointed out in its submission, Governments hold vast amounts of sensitive and personal information and they need to adopt exemplary practices in its management.[136] Thus, the *Commonwealth Privacy Act 1988* contains 11 Information Privacy Principles (IPPs) regulating the collection, storage, use, disclosure and access to, and correction of, one's own personal information by Commonwealth public sector agencies.[137] IPPs 10 and 11 do, however, permit law enforcement use or disclosure of personal information, in recognition that privacy rights must be balanced against other interests, including that the civil rights of the community are helped by maintaining public safety.[138] The Federal Privacy Commissioner noted that these exemptions are included in the Act in recognition that the community clearly wants to be protected from crime, and is willing to concede powers to the law enforcement community.[139]

1.158 In any discussion on expanding police powers, and more specifically in this case in relation to providing law enforcement with the latest technological tools with which they can catch criminals, a delicate balance has to be struck between the privacy rights of citizens and the public interest in maintaining law and order in our community. The Committee has already made recommendations in relation to the issue of the appropriate legislative response and which include full and proper accountability measures. It remains necessary only to make a specific recommendation in relation to the need for the role of the Ombudsman to be expanded in the interests of a consistent approach to accountability.

Recommendation 8: That the Commonwealth Ombudsman's jurisdiction over the use by Commonwealth law enforcement agencies of telecommunications interception be expanded to include the use of any electronic surveillance device.

Conclusions

1.159 New technology is unquestionably a major aid to both criminals and law enforcement services alike. The rapid advance of technology now sees the traditional police officer on patrol in a high-powered car with portable radios and all manner of sophisticated paraphernalia - a far cry from the helmet, whistle and truncheon

---

134 *Submissions,* p. 262.

135 AAP, *Wee Waa's DNA samples go up in smoke,* 20 September 2000.

136 *Submissions,* p. 71.

137 The Victorian Government submission drew attention to its Information Privacy Bill 2000 which was to establish a similar scheme of regulation of the use of personal information in the Victorian public sector - *Submissions,* p. 140.

138 Attorney-General's portfolio, *Submissions,* pp. 195-196.

139 *Submissions,* p. 262.

possessed of an officer 'on the beat' in the not so distant past. At the Customs barrier, traditional methods of manual observation and drug-detecting sniffer dogs have been supplemented by 'Backscatter' X-ray technology, Ionscans and K910B Buster devices.[140] It is clear that such developments in the use of technology are a positive aid to crime control. The prospects for the future are limited only by human ingenuity, with cost reductions, miniaturisation and increasing connectivity offering the benefits of ubiquity and speed.

1.160 Equally persuasive is the argument that if the public and governments have an expectation that their law enforcers will investigate and bring to justice the perpetrators of serious crime, then they should be given access to the latest investigatory tools. Obviously adequate funding holds part of the answer - an area outside the Committee's area of interest. It can, however, give advice to governments about the adequacy of the legislative environment that they have created and in which their officers are expected to operate with maximum effectiveness.

1.161 This Chapter has highlighted the inconsistencies in the national legislative structure which act to thwart efficient law enforcement but which criminals are free to exploit. While in recent years Australian governments have achieved much for which they should be commended, with the development of CrimTrac the most notable example, the Chapter contains a clear call to the Commonwealth, State and Territory Governments to work together on achieving outcomes which are beneficial for all Australians, not simply parochial local interests.

1.162 With goodwill on all sides, positive progress was able to be made in the comparable area of the national regulation of corporations. Harmonisation of State and Territory laws does not require total uniformity, only consistency. That is indeed the basis on which the Committee can call for consideration to be given for TI to be devolved to the States on the one hand without being in contradiction on the other hand with its general proposition that cross-border differences should be eliminated in relation to surveillance device legislation. It may well be, therefore, that the national classification system holds a better precedent for a national law enforcement regime, where all parties have agreed to abide by common national standards, while individually retaining discretion over offence provisions at the State and Territory level. New and emerging technological developments raise many challenges. Governments must meet those challenges cooperatively and proactively.

---

140 See *Submissions,* pp. 202-3 and 241 for detailed descriptions. Mrs Marion Grant, the Australian Customs Service's National Manager, Border Operations, also informed the Committee that a cargo management re-engineering process was underway to make greater use of computer applications, including artificial intelligence systems, in its dealings with importers and exporters - see *Evidence,* p. 54.

CHAPTER 2

MONEY LAUNDERING AND ELECTRONIC COMMERCE

Introduction

2.1 The world has experienced significant economic, political and technological changes in recent years. We have seen a revolution in communications and transport; the deregulation of the financial systems and the development of global markets; and the breakdown of centrally planned economies and their replacement with market oriented ones. This has brought about a massive expansion of legitimate global trade in goods and services and, on the 'crime follows opportunity' principle, it has also facilitated the expansion of crime.

2.2 A regular concomitant of much crime, especially organised crime, is the attempt to legitimise its proceeds. Those proceeds are vulnerable to detection and, potentially, confiscation if they are not 'laundered' and made to appear respectable. Money laundering has come to be seen, not as a relatively victimless crime, but as a significant threat to the economy. As Australian Institute of Criminology researchers Peter Grabosky and Russell Smith described the situation:

> Money laundering is of great concern to law enforcement agencies, and for very good reason. A common strategy for concealing the proceeds of crime entails their investment in and commingling with the assets of legitimate business. The infiltration of legitimate enterprise by sophisticated criminals is a significant threat. Not only can legitimate business provide a convenient cloak or cover for further criminal activity, but the enterprise itself can be exploited and its assets stripped for personal gain, at the expense of investors and creditors. A nation's reputation for commercial honesty could be tarnished by criminal infiltration of legitimate business, with attendant consequence for its overall economic well-being. At the extreme, smaller economies can be seriously distorted by the infiltration of criminal assets, to the extent that the political stability of a smaller state may be threatened.[1]

2.3 Being of an entrepreneurial nature, organised crime seeks to use laundered money to sustain its further criminal activities, which is an added incentive to governments to attempt to prevent it.

2.4 Successive Australian governments have given considerable priority to anti-money laundering activities, as evidenced by the passage of the *Proceeds of Crime Act*

---

1 Grabosky, P. and Smith, R. *Crime in the Digital Age,* Federation Press, Sydney, 1998, p. 175.

1987, the then *Cash Transaction Reports Act 1988*[2] and the *Mutual Assistance in Criminal Matters Act 1987.* Money laundering became an offence in its own right in this country in 1987. Australia was a founding member of the Financial Action Task Force on Money Laundering (FATF), established in 1989 by the G7 group of countries. The NCA also conducted a major study into money laundering techniques in 1991, following a reference from the then Attorney-General.[3]

2.5 As the 1990s progressed, it became clear that the combination of global financial markets, networks for the electronic transfer of money, easy access to financial havens and banking secrecy laws in some countries had the potential to facilitate money laundering. At the request of the then Commonwealth Law Enforcement Board, the Australian Transaction Reports and Analysis Centre (AUSTRAC) formed the Electronic Commerce Task Force (ECTF) to work cooperatively with law enforcement agencies, industry, privacy groups and interested government bodies in identifying emerging electronic commerce issues of potential concern to law enforcement. The task force reported in November 1996[4] and, as noted in the Preface, this Committee's predecessor invited ECTF representatives to discuss the report's findings at a public hearing.

2.6 One of its recommendations was for the formation of an oversight body to handle Australia's entry into the information economy in a holistic manner. The National Office for the Information Economy was established in 1997 within the Communications, Information Technology and the Arts portfolio, with the brief to develop, oversee and coordinate Commonwealth Government policy on electronic commerce, online services and the Internet.

2.7 In July 1997 the Attorney-General set up an Electronic Commerce Expert Group (ECEG) to consider the legal impediments to electronic commerce within the framework of international standards and to report on the form and scope of arrangements for the regulation of e-commerce. Its report was presented in March 1998.[5]

2.8 Technological developments moved so swiftly that a Research Group on the Law Enforcement Implications of Electronic Commerce (RGEC) under the aegis of AUSTRAC was commissioned by the Heads of Commonwealth Operational Law Enforcement Agencies in 1997 to take up where the ECTF left off. In 1999, RGEC produced three reports which have been of inestimable value in shaping the

---

2 In 1991, the Cash Transaction Reports Amendment Act replaced the word 'cash' with 'financial'; the Act is hereafter referred to as the Financial Transaction Reports Act ('the FTR Act').

3 NCA, *Taken to the Cleaners: Money Laundering in Australia,* AGPS, Canberra, 1991.

4 Electronic Commerce Task Force, *Report of the Electronic Commerce Task Force to the Commonwealth Law Enforcement Board,* AUSTRAC, West Chatswood, 1996.

5 ECEG, *Electronic Commerce: Building the Legal Framework* Canberra, 1998.

Committee's thinking on these issues.[6] RGEC has now become the Action Group on the Law Enforcement Implications of Electronic Commerce (AGEC) because it is now charged with putting the results of its research into action.[7]

2.9 In other initiatives, the annual Australasian Police Commissioners' Conference has been active in its efforts to coordinate a national law enforcement approach. It resolved that a National Fraud Desk be established as a secure intranet web site on the ABCI's ALEIN database, which provides law enforcement with up-to-date information on emerging trends and new techniques. It also agreed to establish an Electronic Crime Steering Committee, supported by an Electronic Crime Working Party, to evaluate Australia's capacity to respond to e-crime.[8] In 2000, the Working Party produced a comprehensive scoping paper, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* which the Committee has drawn on considerably in considering appropriate law enforcement strategies for dealing with electronic crime.

2.10 In this Chapter, the Committee will address the broad issues related to money launderering, including the techniques used and the local and international law enforcement arrangements to combat it. It will also consider the development of electronic commerce, its characteristics, level of regulation and potential for abuse. Finally, the Committee will consider the potential for money laundering through e-commerce and whether additional law enforcement measures need to be considered.

Money laundering

Definitions

2.11 Put simply, money laundering is 'the processing of criminal proceeds in order to disguise their illegal origin'.[9] A more elaborate definition is offered in the *Proceeds of Crime Act 1987* (Cth):

> A person shall be taken to engage in money laundering if, and only if:
>
> - the person engages, directly or indirectly, in a transaction that involves money, or other property, that is proceeds of crime; or
>
> - the person receives, possesses, conceals, disposes of or brings into Australia any money, or other property, that is proceeds of crime and the person knows, or ought reasonably to know, that the money or other property is derived or realised, directly or indirectly, from some form of unlawful activity.[10]

---

6 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* West Chatswood, 1999.

7 Ms Elizabeth Montano, AUSTRAC Director, *Evidence*, p. 31

8 AFP, *Submissions*, p. 60.

9 FATF, *The Forty Recommendations*, OECD, Paris, 1990, p. 1.

10 *Proceeds of Crime Act 1987 (Cth),* s.81(3).

Background

2.12 Narcotics trafficking has traditionally been regarded as the single largest source of criminal proceeds.[11] And, as the ABCI points out, illicit drugs and cash are inextricably linked,[12] so the 'proceeds' have usually been in the form of cash.

2.13 In the early days, laundering was achieved by such techniques as 'smurfing', where couriers were employed to go to a large number of financial institutions in order to convert relatively unobtrusive amounts of cash into bank cheques or overseas funds transfers, thereby avoiding the attention which might otherwise have been drawn to a single, substantial cash transaction. Alternatively, the cash was moved out of the country by cash couriers or transmitted via underground banks.[13]

2.14 In its 1991 study into money laundering techniques, the NCA found that the areas most used by money launderers were financial institutions, particularly banks, real estate, and company structures, including cash businesses. Solicitors were used to develop or assist in many money laundering schemes and to send proceeds of crime overseas, particularly to tax havens.[14]

2.15 The NCA study also outlined the most commonly used methods for laundering money at that time. Property or other assets could be purchased in a false name or through a company, purchased for less than their worth, or 'rented' to the money laundering owner. Funds could be deposited into, or moved through, accounts in false names. Funds could be sent overseas by telegraphic transfer, bank draft, travellers' cheques, or physically carried out of the country. Fake deposits could be made, loans to a business owned by the money launderer, or fake debts could be generated. Or funds could be passed through business structures in order to make them appear to be part of legitimate business activity.[15]

2.16 While all of the above techniques are likely to still be practiced, it appears that banking systems, both regulated and underground, remain highly significant vehicles for money laundering.

2.17 Underground banking systems such as 'hawala', 'hui' or 'hundi', 'fei ch'ien' and others have existed for centuries, particularly in Indian, Pakistani, Chinese and east Asian communities throughout the world. They operate on trust. A person wishing to transfer money or value deposits it with the 'banker' (often an ordinary trader) and arranges for its redemption, minus a commission, at an agreed-upon location which is often the business premises of an associate or close relative of the 'banker'. The actual

---

11 FATF, *Annual Report 1999-2000*, Paris, 2000.

12 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, 2001, p. 104.

13 Grabosky, P., *Computer Crime in a World Without Borders,* Paper presented to the 70th Conference of Commissioners of Police of Australasia and the Southwest Pacific Region, Canberra 13 March 2000.

14 NCA, *Taken to the Cleaners: Money Laundering in Australia,* AGPS, Canberra, 1992.

15 ibid., p. ix.

assets need not physically move from country to country, unless required for balancing the books. Such systems are quite legal and are used for legitimate funds transfer, which makes it particularly difficult and culturally heavy-handed to crack down on them. They do, however, have a role to play in money laundering though, by the very nature of that practice, its extent is unknown.

2.18 Australia's multicultural population has ensured that it is an attractive host for such alternative remittance systems. An NCA investigation in 1999 uncovered one such system, operating from retail fabric shops in Melbourne. For a fee, money was transferred between Australia and Vietnam by telegraphic transfer purchased with cash or cheques or via telegraphic transfer via trading companies in Hong Kong and Vietnam.[16]

2.19 The accepted wisdom regarding money laundering suggests that it involves three stages: placement, layering and integration. Placement involves introducing the tainted proceeds into a legitimate context, such as a bank account, without revealing the source of the funds; layering involves moving the assets in a series of transactions to conceal their real ownership and location; and integration involves blending the funds into the mainstream economy, eliminating any indication of tainted origins.[17]

2.20 The initial 'placement' stage is critical for law enforcement authorities, because it presents the best opportunities for detection. Bank accounts still appear to be used by criminal groups to deposit money, often in parcels of less than $10,000,[18] which is the cash transaction reporting threshhold under the FTR Act. The funds are then transferred to overseas accounts, then channelled back into Australia as 'loans' to businesses connected to the launderers. 'Layering' can be achieved by the successive rerouting of funds between bank accounts and corporate structures, which can give the impression of substantial business activity, and is a practice facilitated by the speed of the Internet. 'Integration' will be assisted by the development of stored value systems or electronic cash, to which funds can be downloaded from institutional sources.

2.21 In a recent report on money laundering, the FATF found that these methods continued to be used, along with currency smuggling across borders, the use of such professionals as insurance or securities brokers to assist in laundering schemes, and the use of real estate, gambling, legitimate remittance services and trusts. The international trade in goods and services is also used, both as a cover for money laundering or as a money laundering mechanism itself, by over- or under-valuing goods.[19]

2.22 Emerging trends in money laundering in 1999-2000 in Australia included stock market manipulation, or share ramping. The funds for such transactions are sent

---

16 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, p. 108.

17 Grabosky P. and Smith R., *Crime in the Digital Age,* Federation Press, Sydney, 1998, p. 175.

18 This offence is known as 'structuring'.

19 FATF, *Annual Report 2000-2001,* OECD, Paris, 2001, pp. 15-17.

offshore then repatriated to purchase Australian securities. One case investigated by the NCA involved a Chinese student suspected of laundering money for a narcotics syndicate by using fellow students to remit funds overseas by telegraphic transfer in amounts of less than $10,000.[20]

2.23 The correspondent banking system seems to be increasingly used in money laundering and since the mid-1990s a large number of financial institutions have been registered in offshore tax and financial havens in the Carribean and the Pacific islands. The Cook Islands, for example, with a population of 18,000 is reportedly home to some 3000 separately registered offshore trusts, 1200 registered offshore companies and seven offshore banks; Nauru has some 400 licenced offshore banks; Samoa features 15 offshore banks.[21]

The extent of money laundering

2.24 By its very nature, money laundering is a covert activity, all but impossible to quantify. An effort was made in 1995 when AUSTRAC commissioned Mr John Walker, an independent consultant criminologist, to analyse it. His conclusions were that between $1000 million and $4500 million of Australian proceeds of crime are laundered within Australia or sent overseas. As much as $5500 million may be being sent out of Australia to overseas tax havens, some of which would be from Australian crime and some being overseas crime laundered via Australia, and as much as $7700 million brought to Australia for laundering.[22]

2.25 A 1998 estimate by Mr Michel Camdessus, former Managing Director of the International Monetary Fund, was that between two and five per cent of global GDP would be a consensus range for money laundering worldwide.[23] The Director General of Interpol, Mr Raymond Kendall, had suggested to the Committee in late 1996 that some $450 billion was being laundered per annum worldwide. The need for international action to address illicit activity of this magnitude is apparent.

Domestic anti-money laundering initiatives

2.26 Traditional law enforcement and regulatory attention tended to be directed to the predicate offence, such as the fraud, the drug dealing or the tax evasion. But the value of following the money trail was soon realised, resulting in the passage of the FTR Act.

2.27 The FTR Act requires cash dealers, solicitors and members of the public to report particular financial transactions to the Director of AUSTRAC. Cash dealers are defined broadly to include financial institutions such as banks and building societies,

---

20 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, 2001, p. 108.

21 FATF, *Review to Identify Non-Cooperative Countries or Territories,* Paris, 22 June 2001.

22 Walker, J., *Estimates of the extent of money laundering in and through Australia,* AUSTRAC, Sydney, 1995, p. 41.

23 ABCI, op.cit., p. 105.

insurance companies, futures brokers, managers of unit trusts, firms that deal in travellers cheques or money orders, remittance dealers, casinos, bookmakers and totalisator agency boards. Under the FTR Act cash dealers must report transactions of $10,000 or more, or foreign currency equivalents; they must report all international funds transfer instructions; and they must report any suspicious transaction. Additionally they are required to verify the identity of persons who open accounts or become signatories to accounts. The FTR Act prohibits the opening of an account in a false name. Solicitors are required to report cash transactions of $10,000 or more, while members of the public must report movements of currency of $10,000 or more, into or out of Australia.

2.28 Recent proposed amendments to the FTR Act in Schedule 6 of the *Measures to Combat Serious and Organised Crime Bill 2001* (currently under consideration by the Senate Legal and Constitutional Legislation Committee) extend the definition of cash dealer to include real estate agents and currency dealers, who are potential money laundering channels not currently included under the Act's reporting requirements.

2.29 With funds provided under the National Illicit Drug Strategy, AUSTRAC in 1999-2000 undertook a high risk cash dealer strategy, targetting remittance dealers, bullion sellers and money exchangers. Its audit team conducted 69 audits of such dealers, discovering many instances of non-compliance with the FTR Act in respect of international funds transfer instructions.[24] Just as importantly, such enforcement campaigns also encourage higher levels of compliance in future.

2.30 The number of suspect transaction reports received by AUSTRAC from cash dealers in 1999-2000 was 7,085, a rise of some 500 over the previous year. The majority of reports came from banks, with a small and decreasing number from credit unions, casinos, issuers of travellers cheques and other cash dealers.[25] Analysis of the reports showed that the majority related to tax evasion. Next in numerical significance was structuring, followed by 'unusually large cash transaction', then money laundering, with in many cases the activities being interrelated.

2.31 Suspect transaction reports may, of course, prove to be legitimate activities upon investigation. Nevertheless, AUSTRAC reported that in 1999-2000 the law enforcement agencies to which it reported suspect activity used the information in at least 628 investigations. Uses to which the information was put included: revealing the identities of previously unknown persons and providing links to known entities; confirming addresses; showing associations between targets; analysing movement within Australia and links with overseas countries; and determining the size of criminal enterprises.[26] In the sample cases provided, AUSTRAC's financial intelligence proved particularly useful in tax evasion, narcotics trafficking and people smuggling cases.

---

24 AUSTRAC, *Annual Report 1999-2000,* West Chatswood, 2000, pp. 52-53.

25 ibid., p. 59.

26 ibid., p. 74.

2.32 At the time of the NCA's establishment in 1984, money laundering was not a criminal offence in Australia, it was not illegal to operate bank accounts in false names, there was no Commonwealth or State proceeds of crime legislation and there was no financial transaction reports legislation in Australia. Its legislation was silent on its capacity to investigate money laundering as a 'relevant offence' and its investigations into money laundering were necessarily in conjunction with a predicate offence.

2.33 During the ensuing 17 years of its operations there have been significant changes to the law and administrative practices in Australia relating to money laundering, and the NCA has adapted its role and functions accordingly. In October 1994 the NCA established the Agio Task Force to coordinate the efforts of Commonwealth and certain State law enforcement agencies in the investigation of financial intelligence of suspected money laundering and related criminal activity. In May 1994 the Commonwealth granted the NCA the first of its Limbeck references which enabled the Authority to use its coercive powers to add value to the intelligence information.

2.34 Since July 1997 Commonwealth references - known as Operation Swordfish - have been granted to the NCA to investigate organised revenue fraud (tax evasion, Customs duty and excise evasion), money laundering and predicate offences, including drug trafficking. The *National Crime Authority Legislation Amendment Bill 2000*, currently being considered by the Parliament, includes a proposal to include money laundering as a 'relevant offence' in the NCA Act, which would enable the NCA to apply its special powers directly to such offences in their own right, rather than as an adjunct to another relevant offence.

2.35 Another NCA initiative has been the establishment of a Profits of Crime Case Studies Desk using Intranet technology provided through the ABCI's ALEIN network. Case studies of money laundering and investigative techniques are thus able to be shared among Australian law enforcement agencies.

2.36 The other major stance Australia has taken is to legislate to confiscate the illicit proceeds of convicted criminals, through the *Proceeds of Crime Act 1987* [the POC Act]. While certain fine tuning has taken place, it was recognised that a more major overhaul might be needed to ensure that the basic objectives of the legislation were being met and to comply with Australia's international obligations, including under the Council of Europe *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*. A review of the POC Act was referred to the Australian Law Reform Commission, which produced a report, *Confiscation That Counts,* in 1999, recommending, inter alia, a civil forfeiture regime. In its submission to the Committee, the National Crime Authority was strongly supportive of this recommendation.[27]

---

27 *Submissions,* p. 174.

2.37 On 20 July 2001 the Minister for Justice and Customs, Senator the Hon Chris Ellison, issued an exposure draft of a proposed Proceeds of Crime Bill 2001, which incorporates a civil, or non-conviction based, forfeiture of proceeds of crime. The Minister also indicated that an associated bill would cover revised anti-money laundering offences.

International anti-money laundering action

2.38 The need for international cooperation in the fight against drug trafficking and concomitant money laundering was recognised early in the 1988 Vienna Convention (the United Nations *Convention Against Illicit Traffic in Narcotic and Psychotropic Substances*) and in the 1988 Basle *Statement of Principles* (of the Basle Committee on Banking Regulations and Supervisory Practices on the prevention of criminal use of the banking system for the purposes of money laundering).

2.39 It was the establishment of the Financial Action Task Force on Money Laundering (FATF) in 1989, however, that marked a significant step in international anti-money laundering action. As considered in more detail in Chapter 3, the FATF was established by the then G7 group of countries. It is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering. Such policies aim to prevent proceeds of crime from being utilised in future criminal activity and from affecting legitimate economic activity. Australia was a founding member of FATF; it was also instrumental in the setting up of a FATF-linked regional group, the Asia/Pacific Group on Money Laundering, in 1997.

2.40 In 1990, 40 FATF Recommendations were drawn up to cover all relevant aspects of the fight against money laundering; they were revised and updated in 1996. The 40 Recommendations set out the basic framework for anti-money laundering efforts and are designed to be of universal application. They cover law enforcement and the criminal justice system, the financial system and its regulation, and international cooperation. The recommendations are broad principles for action, for countries to implement according to their particular circumstances and constitutional frameworks. All member countries have their implementation of the 40 Recommendations monitored through a self-assessment exercise and through an on-site examination.

2.41 When the 40 Recommendations were first issued, the focus of many of their preventative measures was on detecting money laundering at the cash proceeds stage. This is reflected in the FTR legislation, which emphasises the reporting of cash transactions of over $10,000. A recent FATF meeting found that, e-commerce notwithstanding, 'cash remains the major if not primary form in which illegal funds are generated today' despite an ever-decreasing reliance on cash by the general public.[28]

28 FATF, *Report on Money Laundering Typologies 2000-2001,* OECD, Paris, 2001.

2.42 The United Nations has also been active in this area. At the 20th Special Session of the General Assembly on the World Drug Problem in June 1998, it adopted a *Political Declaration* and *Action Plan against Money Laundering*, which condemned the laundering of money derived from illicit drug trafficking and other serious crimes and urged all States to implement the provisions against money laundering in the United Nations *Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances* of 1988 and other relevant international instruments. Those provisions included:

- the establishment of a legislative framework to criminalise money laundering through confiscation of the proceeds of crime; and to encourage international cooperation and mutual legal assistance;
- the establishment of an effective financial and regulatory regime to deny criminals and their illicit funds access to national and international financial systems, through customer identification and verification requirements; mandatory reporting of suspicious activity; and removal of bank secrecy impediments; and
- the implementation of law enforcement measures to assist in the detection, investigation, prosecution and conviction of money launderers.[29]

2.43 In 2000 the UN finalised an *International Convention Against Transnational Organised Crime* which requires, among other things, signatories to establish comprehensive money laundering offences under their domestic laws and to adopt detailed measures to combat money laundering.

Electronic commerce

Definitions

2.44 Electronic commerce, or e-commerce, has been defined most simply as 'the use of computers and electronic communications networks to do business'.[30] Every type of business transaction in which the participants prepare or transact their business electronically can be regarded as e-commerce. Some have defined e-commerce more broadly still. The Sacher Group report to the OECD stated:

> Electronic Commerce refers generally to all forms of commercial transactions involving both organisations and individuals, that are based upon the electronic processing and transmission of data, including text, sound and visual images. It also refers to the effects that the electronic exchange of commercial information may have on the institutions and processes that support and govern commercial activities. These include organisational management, commercial negotiations and contracts, legal

29 www.austrac.gov.au/text/recent_news/international_money_laundering/index.htm, visited 27 July 2001.

30 National Office for the Information Economy, *E-Commerce for Small Business,* www.noie.gov.au/projects/ecommerce/SME/index.htm as at 1 May 2001.

and regulatory frameworks, financial settlement arrangements, and taxation, among many others.[31]

Background

2.45 E-commerce as we know it today has burgeoned since the mid-1990s, initially with business-to-business transactions, but now business-to-consumer transactions are taking off.

2.46 This growth has been made possible by the development and rapid uptake of the Internet. Access to Internet services is typically provided by an Internet Service Provider (ISP), a retailer who usually buys wholesale capacity from a telecommunications carrier. While corporate consumers generally connect to the Internet via a data line, residential users can access the Internet via a number of technologies including analogue dial-up, broadband and Wireless Application Protocol (WAP). Dial-up access over the public switched telephone network remains the most common. The computer, telecommunications and broadcast media that can be used to provide mass Internet access are rapidly converging, and thus represent some interesting regulatory challenges for the future.

2.47 E-commerce has the potential to offer many advantages over more traditional commerce, although its use is not without downside risks, as this Chapter discusses. It can empower consumers, giving them more information on which to base their purchase decisions, more choice in their source of supply and a greater ability to demand customised goods and services, and enabling them to conduct their transactions from home. For retailers, it can open up new business opportunities globally and benefits in terms of cost savings.

2.48 The government has signalled its support for e-commerce and made it clear that both e-commerce and the electronic delivery of public services are key strategic areas to be pursued. In December 1997, the Prime Minister responded to the *Investing in Growth* report with a statement committing the Commonwealth government to moving all appropriate Government services online by June 2001.[32] The passage of the *Electronic Transactions Act 1999* ensured that there was no legal impediment to the use of electronic communications to satisfy obligations under Commonwealth law.

Level of e-commerce

2.49 Growth in the most common prerequisite for e-commerce, connection to the Internet, is taking place rapidly. At the end of December 2000 there were 3.9 million Internet subscribers registered in Australia, of whom 3.4 million were household subscribers and 512,000 'business and government'. Together they downloaded 1,050

---

31 Ad Hoc Group of High-Level Private Sector Experts on Electronic Commerce, *Electronic Commerce:Opportunites and Challenges for Government,* OECD, Paris, 1997, p. 20.

32 Attorney-General's portfolio, *Submissions,* p. 195.

million megabytes of data.[33] Forty-six per cent of adult Australians accessed the Internet during the year to May 2000, compared to 41% a year earlier; 33% of households had home access to the Internet in May 2000 compared to 22% in May 1999.[34] Not surprisingly, capital city statistical divisions accounted for the majority of subscribers (74 %); only one per cent of subscribers accessed the Internet via points of presence in remote or very remote regions in Australia.

2.50 Internet access was provided by 696 ISPs at December 2000, down three per cent over the previous quarter, suggesting some rationalisation in the industry. Six very large ISPs, with more than 100,000 subscribers, provided access to 53 % of all Internet subscribers in Australia. Web hosting services were provided by 93 % of ISPs; 49 % provided secure access transaction capabilities. Of the 97,165 business and government web sites, 4,233, or 4 %, provided an environment for secure transactions.[35]

2.51 According to the ninth Australia Online Survey, 46 % of regular Australian Internet users, or 1.6 million people, have tried online shopping in the 12 months to September 2000, with nine per cent of those online shoppers having purchased online more than ten times.[36] In the second half of 2000, Australian retailers captured 68 % of the Australian online spend, up from 45 % in the equivalent period of the previous year. Books remain the most frequently purchased online product, while food and groceries are the clear leaders in repeat online purchases. Sales of CDs, videos, travel and concert or event ticket purchases are building up.

2.52 Other commercial uses of the Internet are increasing: in December 1998, for example, 12 % of regular Internet users participated in Internet banking; by December 2000 that figure had reached 51 %.[37]

2.53 The survey also found that, in December 2000, almost half the regular Australian Internet users had been online for less than two years. The evidence suggests that the levels of participation in Internet transactions such as shopping and banking are heavily influenced by the length of a user's Internet experience, with higher value online transactions not being undertaken in the first two years of Internet use.[38]

2.54 The regular Internet users surveyed continued to express much the same concerns with the Internet as had been shown in previous surveys: computer viruses (22%); response times (13%); security of financial transactions (12%); junk email or

---

33 Australian Bureau of Statistics, *Internet Activity, Australia,* December quarter 2000, Cat. no. 8153.0

34 Australian Telecommunications Authority, *Telecommunications Performance Report 1999-2000,* ACA, Melbourne, 2000, p. 161.

35 Australian Bureau of Statistics, *Internet Activity, Australia,* December quarter 2000, Cat. no. 8153.0.

36 www.consult, *The 9th Australian Internet User Report, July-December 2000,* p. 30.

37 ibid., p. 34.

38 ibid., p. 7.

intrusive marketing (12%); privacy (11%); and cost of Intenet access (10%). When asked what would reassure them about online transactions, 21% indicated that 'guarantees' from banks and retailers regarding transaction security would be helpful.[39] Of the non-purchasers online, 35% gave as their reason that they did not trust the Internet with their credit card details. The online purchasers did so for a variety of reasons: 29% cited convenience; 13% to save money; 13% to buy goods unavailable in Australia; and 10% to save time.[40]

2.55 Statistics from the United States show that almost 20 million US households shopped online in December 2000, spending in total US$6.1 billion, with the average per household spend US$308.[41] Forrester Reseach estimates that worldwide net commerce will rise from US$657 billion in 2000 to $6.8 trillion in 2004, with the Asia-Pacific region accounting for about a quarter of that figure.

Features of e-commerce

2.56 E-commerce has a global spread, it is open to all with an Internet connection, it is convenient, and it is immediate. One can pick and chose from a vast array of goods and services from all around the world, compare prices and quality, and effect a purchase with the click of a mouse from the comfort of home, 24 hours a day, seven days a week. Transactions occur in real time, with the vendor being paid immediately

2.57 But e-commerce has other features which are more challenging. It uses the Internet, an unregulated medium, broadly speaking, and one which has attracted a new breed of offender, the cyber-criminal. Its success is reliant on the use of cryptography to ensure the security of financial transactions. It removes the certainty of knowing who you are dealing with, for both purchaser and vendor. And it means that your private details are more widely known than before.

2.58 E-commerce has the potential to bring about change on an unprecedented scale. In this report, the Committee will not consider matters such as the impact of e-commerce on the economy as a whole, nor its social or political ramifications, important though they may be. It will concentrate on those features of e-commerce which may be susceptible to crime, including money laundering, and consider the implications for law enforcement.

E-commerce challenges and responses

2.59 E-commerce is expanding at an exponential rate. This suggests that for the present, both purchasers and vendors are sufficiently convinced of its relative security or, at the least, reassured that the benefits outweigh the possible risks. Those risks relate primarily to the medium of the Internet with its anonymity, speed and geographic spread, and include: the relative ease with which identity fraud can be

---

39 ibid., p. 44.

40 ibid., p. 47.

41 Forrester Research Online Retail Index, www.forrester.com

perpetrated; the likelihood of external hacking, denial of service or spamming attacks to e-commerce web sites; the authentication of e-commerce web sites; the concealment of communications with cryptography; and the security of payment systems. Many of the core issues are not unique to the electronic world, but may present new challenges in that context, and require different responses. The Committee examines these features in the following sections.

Geographic spread

2.60 When things go wrong, e-commerce may present jurisdictional challenges because of its global spread. Consumer protection laws vary greatly from country to country and it might be impossible to locate an organisation comparable to Australian fair trading or consumer affairs bodies to assist.

2.61 A typical scenario might be as follows. Australian company XXX establishes a commercial web site in the USA, for faster access and lower costs. It advertises widgets, with an extensive online catalogue and online payment facilities. It software accesses backend supply databases in London, Rome and Buenos Aires, and it has arrangements with couriers to deliver its widgets anywhere in the world. The companies whose credit cards XXX accepts issue invoices to its participating banks from regional headquarters in, say, Malaysia.

2.62 Such a convoluted scenario is the norm in e-commerce. When and if criminal conduct occurs along the way, interesting legal questions are raised. If, for example, in the scenario above, a New Zealand customer orders and pays for 100 widgets and fails to receive them because they are stolen somewhere en route, where does the offence take place? Which jurisdiction is responsible for dealing with it? What laws, if any, cover the offence in the jurisdiction in which it occurred? What evidence of the transaction is available and is it acceptable to the relevant court? In some circumstances, but not all, law enforcement agencies may be able to assist victims through recourse to mutual assistance arrangements (as described in Chapter 3) but for low-level offences assistance is unlikely to be a law enforcement priority.

2.63 The question of jurisdiction has been actively canvassed at international level. In particular, the Council of Europe *Draft Convention of Cyber-Crime* is a significant step towards the harmonisation of laws relating to computer-related crime, addressing as it does the substantive criminal law, search and seizure of electronic data, jurisdiction and mutual assistance.

Speed

2.64 E-commerce can be conducted instantly. For the private purchaser, this is one of its attractions; for the vendor, it may present problems especially in the automated sales area or inventory-and-dispatch systems. While most vendors employ automated scanning and verification procedures, they may not detect high-volume, low-value frauds which can be speedily effected on the Internet.

2.65 The Internet, with its multiplier effect, facilitates email spam and denial of service attacks, in which thousands of emails can be routed through a third-party server for distribution worldwide. When directed at an e-commerce site, the damage can be dramatic.

2.66 These are the risks involved in participating in e-commerce and should be managed as such. High-level preventative IT security is an obvious answer for the private sector, rather than reliance on law enforcement assistance.

Anonymity

2.67 In traditional business dealings, customers build up relationships over time with retailers where familiarity, experience and a bricks-and-mortar presence all added to the security of business dealings. But a feature of e-commerce is that of separation. Buyer and seller may never meet in the real world and have no direct means of knowing who they are really dealing with. While the loss of face-to-face contact and the resultant loss of collateral information introduces an element of risk into e-commerce transactions, it is important to remember that mail order and telephone order transactions, with not dissimilar features, have been in operation successfully for some years.

2.68 Anonymity can be further enhanced by the use of anonymous remailers. As the name suggests, these are e-mail servers which strip off e-mail headers and onforward the message to the intended recipient, either anonymously or, if a response is required, with a pseudonym. Some remailers provide encryption services in addition to mail forwarding. And users who do not trust the remailers can of course forward their messages through multiple remailers. It has been suggested that remailers can batch messages so that, if a law enforcement agency intercepted them, it would not be able to deduce who was talking to whom.[42]

2.69 It is of course possible, in the investigation of potentially criminal conduct, for law enforcement to trace, with the assistance of ISP records, the Internet address or domain name from which a particular message was sent, and to discover the name of the person responsible for maintaining that domain name, but not to identify the user at the time.

2.70 The issue of identity is complicated because it is technically possible for a fake web site to masquerade as another, a practice known as 'spoofing'.[43] Individuals too can mask their identity by 'looping' and 'weaving' through a number of previously compromised systems.

---

42 Denning, D. and Baugh, W.E. 'Hiding crimes in cyberspace', in Thomas D. and Loader B.D. (eds), *Cybercrime: law enforcement, security and surveillance in the information age,* Routledge, London, 2000, p. 125.

43 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood, 1999, p. 42.

2.71 For e-commerce to succeed, one of the imperatives is for parties to transactions to be sure of the identity of the person or site they are dealing with. Cryptography, or the practice of transforming the contents of a message to a form that cannot be decoded by unauthorised persons, is the generally preferred solution. A commonly used form is public key cryptography, which works as follows. Person A wishes to send a secure message to person B, so firstly A encrypts the message with B's public key, then 'signs' it with A's private key. B receives the message which is notionally from A and verifies that it is from A by decrypting it using the only key which will do so, namely A's public key, then decrypts the contents using B's private key.[44]

2.72 Public key cryptography is readily available software and the use of digital signatures increases confidence levels in the authenticity of a transaction. Without a biometric component, however, there will always be an element of doubt. For the time being, biometric identifiers such as fingerprint recognisers or iris scanners are relatively expensive and have not gained widespread acceptance. This can be expected to change should commercial demand make it viable.

2.73 Public key cryptography is equally available to money launderers and other criminals as it is to those seeking merely to communicate securely and privately for commercial reasons. Given the strength of even the commonly available cryptographic algorithms (with key lengths of 128 bits or more) law enforcement agencies world-wide have sought legislative leverage to compel access to keys, rather than engage in expensive and time-consuming and, at times, fruitless efforts to 'crack' the encryption. This matter is further considered in Chapter 1.

2.74 While it is generally agreed that encryption poses a potential threat to law enforcement agencies, the Committee is not aware of evidence of the actual extent of its use by criminals in Australia. The FBI's Computer Analysis Response Team began collecting such data in April 1998 and by December of that year, only four per cent of forensic cases handled involved the use of encryption.[45]

2.75 In terms of the problem for e-commerce of anonymity, public-key based, crypto-secured digital identification should provide a high level of confidence in transactions, but it may not do a great deal to assist law enforcement agencies. Legitimate and illegitimate commerce can exist side by side. The computer networks of large organisations are generally protected by firewalls against external security breaches, but this also means that individual Internet users may be represented externally by a single Internet Protocol (IP) number, thus complicating the identification process unless firewall logs are kept. And even if it is possible to identify the physical location of a computer with a particular IP number, it may run a

---

44 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, pp. 42-43.

45 Denning, D. and Baugh, W.E. 'Hiding crimes in cyberspace', in Thomas D. and Loader B.D. (eds), *Cybercrime: law enforcement, security and surveillance in the information age,* Routledge, London, 2000, p. 112.

multi-user operating system, with identification only possible if users have a separate login ID.

2.76 The Committee notes that at present, there appears to be no requirement for entities that trade electronically to identify themselves other than by their URL. The RGEC report noted that the Australian Taxation Office was unable to locate owners of 15 % of businesses with com.au domain names.[46]

Identity fraud

2.77 Knowing who you are dealing with electronically is further complicated by the ease with which a false identity can be achieved. As the Office of Strategic Crime Assessments (OSCA) has noted, technology has weakened the integrity of many identifiers currently in use.[47] False identity papers can be readily acquired through the Internet: a number of web sites offer near-authentic forgeries of official documents, which can in turn be used to facilitate money laundering and other crimes. The NCA expressed particular concern about the registration of business names in false identities, SIM cards and mobile phones in false names, and forged or false credit cards, and, while acknowledging the difficulties in verifying the authenticity of identification documents, it also expressed its concern at the apparent readiness of private and public sector bodies to accept identity documents at face value.[48]

2.78 Proof of identity is required in Australia for such commercial activities as opening a bank account or registering a company. Birth certificates are often required. The banks are acutely aware of the difficulties and have undertaken research into the extent of the problem. Westpac and the NSW Registry of Births, Deaths and Marriages undertook a pilot study of a certificate validation service, finding that some 13% of birth certificates provided as part of the identification documentation were false.[49]

2.79 The problem is compounded by the fact that once one agency accepts the false documentation and issues, for example, a driving licence or a company number, those readily verifiable details will assist the false identity holder to build up a portfolio of 'proofs'. Even the '100 Point' system of identity verification used by a range of Commonwealth agencies is vulnerable to abuse from the use of forged or stolen identity documents and such is the range and source of possible documents being presented that organisations' abilities to check are limited.

---

46 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, p. 50.

47 OSCA, *The Changing Nature of Fraud in Australia,* Canberra, 2000, p.10.

48 NCA, in *Submissions,* p. 166.

49 House of Representatives Standing Committee on Economics, Finance and Public Administration, *Numbers on the Run,* 2000, p. 67.

2.80 The extent of the use of identity fraud is, by its nature, impossible to quantify. In one 1999 survey of 1800 large Australian companies, KPMG found that 11.9% of fraud incidents involved the use of false documentation.[50]

2.81 In one widely-reported American case, touted as 'the largest ID theft in Internet history', a Brooklyn busboy named Abdullah, using computers in a local library, duped companies into providing credit reports on more than 200 of the celebrities, millionaires and corporate executives listed in Forbes magazine. He then used the confidential data to clone their identities and gain access to their credit cards at accounts at some of the most prestigious brokerage houses and investment banks.[51]

2.82 While technology has augmented this problem, technological devices also offer perhaps the best prospect for limiting certain kinds of identity fraud. User identification systems which involve security devices incorporating unique biometric identifiers are already available: keyboards and mice containing fingerprint scanners, for example.[52] Space geodetic methods can be used to pinpoint the physical location of computer users. And single-use passwords, challenge-response protocols and call-back systems can also be used to carry out user authentication.

Security of payment systems

2.83 Another aspect of e-commerce which discourages potential online shoppers is the question of whether the payment system is secure. In Australian-based e-commerce, pre-existing credit arrangements such as credit and charge card schemes are still the most common payment form for purchases via the Internet, with purchasers quoting a card number, protected by encryption. These schemes, being global, facilitate international transactions involving currency conversions, but are capable of abuse: the payer can repudiate the transaction; and card numbers can be fraudulently obtained.[53]

2.84 The perception is that credit cards can be easily intercepted on the Internet and misused. This has certainly occurred. The ABCI told the Committee of numerous recent incidents of organised Asian criminal syndicates 'skimming' electronic data off legitimate credit cards and encoding the information on stolen or counterfeit cards, which are then used to purchase goods. An investigation in New South Wales, Operation Massat, resulted in the dismantling of a highly organised Malaysian based

50 ibid., p. 75.

51 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 5.

52 Grabosky P., Smith R. and Dempsey G., *Electronic Theft: Unlawful Acquisiton in Cyberspace,* Cambridge University Press, 2001, p. 195.

53 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, p. 59.

syndicate involved in approximately $50 million counterfeit-related fraud in 1998 and 1999.[54]

2.85 It appears that much credit card fraud on the Internet comes from apparently valid credit card numbers generated by software programs. When the charges are small, the likelihood of full authorisation checks being performed is limited; checking would disclose that the card numbers were fraudulent.[55]

2.86 Research into credit card losses in the online retail industry has shown mixed results. ActivMedia found that 'chargebacks' amounted to only 1.22 %, as opposed to 1.47 % offline.[56] This is well within the average business risk most retailers would accept. Other reports have suggested otherwise, however. It has been reported that a website operated by Harvey Norman was shut down because a quarter of the orders placed on it were on stolen credit cards.[57] A UK report found that e-commerce firms were reporting up to 25% of online transactions as fraudulent, with an average of 5%.[58] Yet another source reported overall fraud rates of 0.08 to 0.09 %, with little difference between face-to-face and mail-order/telephone-order transactions and electronic transactions.[59] Whatever the exact level, it is clearly a matter which will self-regulate, with merchants refusing to accept credit card payments if they become too unreliable.

2.87 From the point of view of the customer, most financial institutions offer their customers a measure of protection against fraudulent use of their credit card. So long as the unauthorised transaction is reported immediately, banks will usually not hold the cardholder liable, or will limit liability. Similarly, if the goods fail to arrive or are returned because they are faulty, banks may reverse the payment to the business.

2.88 Credit card numbers or other payment details are encrypted before being transmitted over the Internet. Both Netscape Navigator and Microsoft Internet Explorer use a method known as Secure Sockets Layer (SSL) to encrypt data before transmitting it, and show a lock or an unbroken key in the browser window. But SSL does not serve to authenticate either transacting party.

2.89 The major card issuers and financial institutions have been developing a process to provide both advanced encryption, combined with a system of digital certificates provided by card issuers, known as Secure Electronic Transaction (SET).

---

54 *Submissions,* p. 127.

55 ACS & NOIE, *The Phantom Menace: Setting the record straight about online credit card fraud for consumers,* [2000].

56 ibid.

57 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 4.

58 ibid.

59 ACS & NOIE, *The Phantom Menace: Setting the record straight about online credit card fraud for consumers,* [2000].

SET would enable the identity of the cardholder and the merchant to be authenticated, while ensuring that neither the merchant nor the cardholder's bank sees the purchaser's credit card number. The RGEC report suggested, however, that SET was proving difficult to deploy.[60]

2.90 Given the level of concern about security of credit card payments, and the reluctance of some payees to accept payment by credit card because of the fees charged, alternative forms of payment, such as direct debit schemes, are developing. Many banks have begun providing Internet bill payment facilities, for example. A third method is the stored value scheme, by which purchasers pay for value in advance either on a smartcard or on a computer; the value is progressively depleted until it runs out and is topped up again.

2.91 The smartcard in particular was heralded as the replacement for cash for small purchases but has been slow to take off. It has been suggested that banks are reluctant to support stored value schemes for fear of losing fees from EFTPOS and credit cards, while merchants are either waiting for the critical mass to be generated to make the expenditure associated with implementing such schemes worthwhile or they are implementing private stored value schemes such as TAB accounts and pre-paid SIMs for mobile phones.

2.92 It has also been suggested that the smartcard future may depend on its adoption for multiple purposes, such as personal identification and access to services.[61] Both Germany and Spain have gone down this route, but Australia with its history of cultural aversion to the carrying of identity papers, as evidenced by the failure of the Australia Card proposal in the 1980s, is unlikely to follow suit.

2.93 There are Internet variations on the smartcard theme, variously called e-cash, Digicash or cybercash, where funds are deposited in a personal bank account and then transferred to the e-cash system which generates and validates e-cash for use on the Internet. The ABCI reported that only one Australian bank offered such a service.[62]

2.94 Internet payment schemes are in a state of evolution and it is difficult to predict which will become the norm. What is clear is that private stored value schemes operated by non-bank financial institutions outside the regulated financial sector could provide systemic risks for the financial sector.[63]

---

60 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, p. 61.

61 Ad Hoc Group of Hi-Level Private Sector Experts on Electronic Commerce, *Electronic Commerce: Opportunities and Challenges for Government,* OECD, Paris, p. 36.

62 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, 2001, p. 105.

63 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1., West Chatswood,, 1999, p. 63.

Computer system attacks

2.95 While e-commerce is dependent on the Internet, there is always a potential threat from computer network break-ins. The FBI has defined three types of cyber-criminal engaged in such activity: 'crackers', who seek intellectual stimulation from their activity; vandals, seeking revenge; and those who commit fraud, damage computer systems or undertake espionage.[64]

2.96 The recreational hacker or cracker is often out to find bugs or holes in computer security systems and may rearrange or deface web pages. Government sites can be attacked to make a political point, as was the case when US, UK and Australian servers were systematically defaced by 'Pentagard' in January 2001.[65] A small subset of hackers are more malicious and can cause damage through many techniques: denial of service attacks (swamping a commercial web site with so many emails that it cannot cope); computer viruses; the damaging, deleting or erasing of files; and making public confidential information. Still others go on to minor fraud, such as using stolen credit card information to make purchases, or other non-commercial crimes such as cyberstalking or child pornography.

2.97 A number of studies have looked at cyber-intrusion and the perpetrators thereof. A joint 1997 OSCA-Victoria Police survey of computer crime in a representative sample of over 300 Australian companies found that 37% of its sample experienced intrusion or unauthorised use of its computer systems, 90% of which was by insiders.[66] Similar results emerged from a follow-up survey of 350 companies in 1999 by Deloitte Touche Tohmatsu and Victoria Police. One-third of the companies reported an IT attack in the previous 12 months; 83% of intrusions were internal and 58% external; losses exceeding $10,000 occurred in 12% of the attacks; and it was thought that the attacker was most likely to be a disgruntled employee or independent hacker.[67] Of course, internal fraud and retaliatory action of this kind has always been with us - only the methods may now differ. It is usually handled in-house and not often brought to the attention of law enforcement. In the latter survey, for example, 42% of companies attacked did not report the incident outside the company.[68]

2.98 The Australian Computer Emergency Response Team (AusCERT), an operational arm of the University of Queensland and Australia's peak agency assisting in the prevention of computer-based attacks, received 8,197 computer security

---

64 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, p. 23.

65 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 4.

66 OSCA and Victoria Police, *1997 Computer Crime and Security Survey,* pp. 15-17.

67 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 6.

68 ibid.

incident reports in 2000, an alarming increase over the 1,816 of the previous year.[69] The 'incidents' were largely viruses, distributed denial of service attacks or network scans.

2.99 Further evidence of the growth in cyber attacks comes from the annual US Computer Security Institute/FBI Computer Intrusion Squad computer crime and security survey. This survey of information security professionals attracted only 643 responses in 2000 (a 15% response rate) and its results perhaps should not be extrapolated to the cybercommunity as a whole. That said, it disclosed that 70% of respondents experienced unauthorised use of computer systems in 2000; 25% detected system penetration from outside; 27% detected denial of service; 71% detected unauthorised access by insiders; 85% detected viruses; 11% detected financial fraud and 17% detected sabotage of data and/or networks.[70] Financial losses to the 273 respondents who were prepared to report them totalled US$265,589,940.[71] Of the 43% of respondents who conducted electronic commerce on their site, 19% suffered unauthorised access or misuse; 64% reported website vandalism; 60% reported denial of service; 8% reported theft of transaction information; and 3% reported financial fraud.[72]

2.100 One Australian example of the type of computer attack undertaken, and the outcome, is of interest. A 27-year old male known a 'Optik Surfer', who had been working as a computer networking consultant, was refused employment by an ISP. He obtained access to the company's computer network by using the technical director's user account and password, accessed the subscriber database, showed various journalists those subscribers' credit card details, and left a message on the company's home page that its security system had been compromised. The company lost more than $2 million, was required to change its business name and sold off its Internet access business.[73]

2.101 A more recent security breach involved the government's GSTAssist website, when a student, known variously as 'Kelly' or 'K2', was able to access the records of more than 20,000 GST-registered providers and emailed their confidential details to some 17,000 of them.[74]

---

69 ibid., p. 7.

70 Power R., '2000 CSI/FBI Computer Crime and Security Survey', *Computer Security Issues and Trends,* 6(1) Spring 2000, p. 5.

71 ibid., p. 6.

72 ibid., p. 10.

73 Smith, R.G., 'Internet-related fraud: crisis or beat-up?', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 9.

74 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 5.

2.102 How frequently such cases occur is difficult to determine. While there has been considerable media excitement over the hacker phenomenon, the AFP has been involved in relatively few hacking investigations, prompting one Federal Agent to question whether high-volume, low-level hacking attempts were a portent of global catastrophe or merely the high-tech equivalent of someone rattling a locked door.[75]

2.103 Companies have a vested interest in not disclosing that their computer security has been compromised. It may be, as Dr Russell Smith of the AIC has suggested, that the instances of computer fraud are relatively few in comparison with the volume of transactions and that the media, criminal justice personnel, the computer security industry and others all have a vested interest in portraying the problem as more serious than it is.[76]

2.104 The hacking phenomenon is being addressed in the Government's Cybercrime Bill 2001, currently before the Parliament. The Committee recognises its importance in the e-commerce and general crime sphere but will not pursue the topic further as its direct relevance to money laundering is limited.

Regulation of e-commerce

2.105 Since the inception of e-commerce, debate has raged over the level of regulation it requires. In Australia the Information Industries Task Force recommended that what was needed was a non-regulatory, market-oriented approach that would facilitate the emergence of a predictable legal environment to support business and commerce.[77] Given the global nature of e-commerce, what is clear is that Australia must conform with international norms or be left behind.

2.106 In 1996, the United Nations Commission on International Trade Law (UNCITRAL) developed a Model Law on Electronic Commerce, an international legislative template intended to harmonise domestic legal approaches to e-commerce. The Attorney-General set up an Electronic Commerce Expert Group (ECEG) to consider the Model Law's applicability to Australia and any legal impediments to e-commerce here. The ECEG reported in 1998, recommending the enactment of Commonwealth electronic commerce legislation based on the principle of technology neutrality, broad in its operation, and which would remove any legal impediment to a person's use of electronic communications to satisfy legal obligations under Commonwealth law. The recommendations were put into effect via the *Electronic Transactions Act 1999* (Cth) and a national approach encouraged via the development with all States and Territories of a uniform Electronic Transactions Bill.

---

75 Guerts, J., 'fraud@internet.com.au', *Platypus,* March 2000.

76 Smith, R.G., 'Internet-related fraud: crisis or beat-up?', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, pp. 3-4.

77 Information Industries Task Force, *The Global Information Economy: The Way Ahead,* 1997, pp. 71-74.

2.107 The legislation has been described as creating 'a light handed regulatory regime'.[78] Significantly, while it deals with the threshold issue of the legal recognition of electronic signatures, it does not impose a particular authentication framework. The ECEG specifically rejected a public key authentication framework as proposed by Standards Australia and endorsed by the Wallis Inquiry.[79] It did so principally on the grounds of the volatile state of the authentication technology and a desire not to 'pick winners' among, for example, retinal scans, 4-digit PINs and private keys based on assymetric key cryptography. Yet as para. 2.150 details, the Commonwealth Government has proceeded with a voluntary accreditation process in its Gatekeeper Project.

2.108 E-commerce does place a significant amount of personal information in the hands of merchants, information of considerable commercial value. To counter its inappropriate use, the government has amended the Privacy Act to include national privacy principles which will apply to most private sector organisations from 21 December 2001.[80]

2.109 Rather than regulate, the government's approach to e-commerce has been to emphasise consumer education and awareness raising. That such an approach is needed was emphasised by an experiment conducted by ASIC, which set up a spoof millenium bug insurance site that managed to persuade 233 people to be prepared to part with more than $4 million.[81] The kindest interpretation is that the use of technology may give an appearance of legitimacy to what would otherwise be simple fraud.

The money laundering potential of e-commerce

2.110 It is the view of law enforcement agencies both in Australia and overseas that the Internet and e-commerce technology will be primary channels for committing financial crimes.[82] The AFP cited cryptography, the lack of borders and electronic payment systems as the characteristics inherent in e-commerce that will facilitate money laundering.[83] Amongst other reasons for expecting money laundering to increase, the FATF pointed to the growing number of offshore banking and tax minimisation services offered via the Internet; the anonymity provided by Internet banking services; the lack of audit trail through the use of unregulated cyberbanks and credit card processing facilities in tax havens; ready access to counterfeit

78 Attorney-General's portfolio, *Submissions,* p. 217.

79 ECEG, *Electronic Commerce: Building the Legal Framework,* 1998, p. 136.

80 *Privacy Amendment (Private Sector) Act 2000.*

81 Guerts J., 'fraud@internet.com.au', *Platypus,* March 2000.

82 NCA, *NCA & Cybercrime: scoping paper,* June 2000, p. 6.

83 *Submissions,* p. 62.

indentification; access to encryption for secure communications; and an enhanced capacity to move money via smart cards and e-cash.[84]

2.111 While most authorities agree that the e-commerce infrastructure has the potential to assist in the laundering of criminal proceeds, the extent to which it is currently being used to do so is unclear. In the AFP's view, 'e-money laundering is thought to be negligible, for now',[85] and Tasmania Police found it 'not apparent' in that State.[86] While Victoria Police saw that e-cash and e-banking would provide launderers with future opportunities, it has not to date detected significant organised crime usage of computer systems to launder money; rather, the major detected cases related to extortion and the planning of crimes.[87] The NCA also noted that few cases had come to its attention of organised crime groups exploiting e-commerce and Internet banking.[88]

2.112 It may be that law enforcement has failed to detect such activities or, and more probably in the view of the Committee, e-commerce participants or financial institutions have not reported their losses for fear of repercussions in the market place.

2.113 In its scoping paper, the NCA outlined a case which did come to light. Two 18 year old boys in the Welsh town of Dyfed-Powys were charged with breaking into electronic commerce Internet sites in five countries and stealing information on 26,000 credit card accounts. The investigation involved the United States Federal Bureau of Investigation, the Dyfed-Powys Police Service and the Royal Canadian Mounted Police. According to an FBI spokesperson, the boys were alleged to have hacked into nine e-commerce web sites in the United States, Canada, Thailand, Japan and the United Kingdom; losses were estimated at approximately US$3 million.[89]

2.114 To what extent *organised crime* is exploiting the potential of e-commerce for *money laundering,* as opposed to individuals exploiting the potential of e-commerce for individual gain, or revenge, or amusement, is even more difficult to ascertain.

2.115 When money laundering techniques are considered in parallel with e-commerce realities, a number of possible challenges become clear. The use of cryptography has an equal potential to assist criminal communications as it has to secure legitimate transactions. While new technology can be employed to good effect to assist in the tracing of communications, electronic evidence is relatively easy to destroy. E-commerce has a global reach and individual jurisdictional laws could be exploited by money launderers living in one jurisdiction, perpetrating offences in a

---

84 FATF, *Report on Money Laundering Typologies 1999-2000,* OECD, Paris, 2000.

85 *Submissions,* p. 63.

86 *Submissions,* p. 43.

87 *Submissions,* p. 55.

88 *Submissions,* p. 162.

89 NCA, *The NCA and Cybercrime: Scoping Paper, June 2000,* p. 27.

second jurisdiction and transferring value through many other jurisdictions. And although it is perhaps too soon to tell which of the new electronic payment systems will become most widely used, and which user identification techniques will develop, they all present some possibility of exploitation by criminal elements for money laundering and other purposes.

2.116 Of particular concern is the potential of the stored value card to assist in money laundering. If stored value technology becomes widely accepted, it will present a considerable threat, particularly if the value stored is high. In a way not dissimilar to high-value banknotes today, highly portable stored value cards could facilitate money laundering. Some stored value systems have detailed audit trails because fund transfers are effected through regulated financial institutions; others, such as the UK Mondex system, might have only limited audit trails.[90] If e-commerce begins to operate outside of the regulated financial system, transactions are essentially untraceable. Alternative forms of digital cash may cause similar concerns.

Next steps

2.117 Policing of cyberspace raises some interesting challenges for the global community, not only for law enforcement. The approach to crime control will be, perhaps more than ever, a shared responsibility among law enforcement agencies, the e-commerce and IT industries themselves and the individual user. The view put forcefully to the Committee by representatives of the Attorney-General's Department was that 'the first line of defence should be self-defence';[91] that effective protection from threats within the electronic environment will require risk management strategies by the private sector and private individuals, albeit with government and law enforcement agency encouragement and assistance.[92]

2.118 However, having taken a positive role in promoting e-commerce, the government clearly has a duty to ensure that the public can engage in e-commerce safely and with confidence that, in the event of major mishap or misuse, law enforcement agencies are able to step in. Various provisions to achieve this were advanced during the Committee's inquiry. The AGEC Action Plan, which was warmly supported by the NCA, called for the following key issues to be addressed:

- develop joint public and private sector strategies to raise awareness and manage risks associated with the information economy;
- improve IT skills in the public and private sectors;
- develop appropriate interception, computer forensics capabilities;
- advocate appropriate levels of electronic authentication;

---

90 ABCI, *Australian Illicit Drug Report 1999-2000,* Canberra, 2001, p. 105.

91 *Evidence,* p. 29.

92 *Evidence,* p. 26.

- facilitate appropriate record-keeping standards for ISPs; and,
- effective administration of mutual assistance and extradition arrangements.[93]

These are all sensible suggestions. The Committee has considered interception capabilities and the possible regulation of ISPs in Chapter 1; it addresses mutual assistance and extradition matters in Chapter 3. In the remainder of this Chapter it considers in particular the matters of awareness-raising, public-private sector partnerships, electronic authentication, and whether a computer forensics capability is required. It also looks briefly at whether there is a role for government in regulating access to electronic tools of crime such as strong cryptography.

Awareness-raising

2.119 Several witnesses took the view that, to a considerable extent, responsibility for preventing e-crime lies with e-commerce participants themselves. Just as car theft is discouraged by the owner taking precautions such as locking doors and fitting immobilisers, so e-commerce participants should engage in target-hardening practices.

2.120 From the business point of view, these could include appropriate levels of IT security, a preparedness to verify customer identity and to deal only with properly authenticated businesses, all of which would have the added benefit of reducing any money laundering potential of e-commerce.

2.121 From the point of view of the individual customer, again the question of appropriate IT security applies, but equally it is a case of *caveat emptor,* or buyer beware. Customers should be prepared to check on the credentials of Internet companies before they entrust them with their orders and credit card details, just as they do when choosing to buy through mail order.

2.122 The Police Commissioners' Conference Electronic Crime Strategy recognises a role for police in awareness-raising. One of its objectives is to 'create a safer community by contributing to community education about electronic crime, cyber ethics and how best to avoid victimisation';[94] key activities are to produce and deliver crime prevention information detailing how to avoid or minimise victimisation and to support private organisations in the production of consistent and useful consumer protection information.

2.123 Other government agencies have already taken practical steps to bring these matters to general attention. NOIE, through its 'Shopping Online?' project, has produced a useful series of consumer awareness publications on the risks and benefits of online shopping.[95] To overcome the problem of cross-border Internet fraud, a

93 *Submissions,* p. 147.

94 ACPR, *Electronic Crime Strategy of the Police Commissioners' Conference Electronic Crime Steering Committee 2001-2003,* 2001, p. 15.

95 www.noie.gov.au/projects/consumer/shopping_online/index.htm

multilingual website www.econsumer.gov is proposed, to provide information on consumer protection laws in 13 countries and offer consumers a way to file complaints online. The cooperating governments will use a parallel, but secure, site to share complaint data and information on e-commerce fraud investigations. Australia's participation is through the ACCC.[96]

Public-private sector partnerships

2.124 New technologies may provide the means by which e-crimes such as fraud and money laundering are facilitated, but they can also be expected to furnish the means by which such crimes will be able to be detected. AUSTRAC's use of artificial intelligence to pinpoint suspect transactions below the reporting threshold is a case in point.

2.125 It is generally accepted that the newest technology and the greatest IT expertise resides in the private sector, for the simple reason that the private sector has most to gain from its commercial exploitation and has fewer constraints in paying for it. As Mr Murray Rankin, of the private sector firm, The Distillery, told the Committee:

> a lot of the potential [public sector] users of private sector products take the decision to use what would arguably be inferior products because of things such as budget constraints ... They are prepared to accept a lesser service at a cheaper cost ...[97]

2.126 Criminals are using advanced technologies to commit crimes, as the ABCI illustrated with the case of the 'Post-card Bandit', Brendan Abbott, who was in possession of a small arsenal of technological aids when apprehended.[98] Law enforcement has always faced an enormous challenge in terms of keeping up with the technology available to the better-resourced criminals. Given the specialist nature of some of the latest technology, and its relentless and rapid advance, the only real option for government in general, and law enforcement in particular, is to enter into increasing partnership with the private sector in terms of both technology and expertise.

2.127 There appears to be little consensus, however, on the format such public-private sector 'partnerships' might take. At one end of the spectrum, there are jointly funded and operated cybercrime agencies; at the other, there is the employment of private sector experts in public agencies on contract. In the middle, there are 'partnerships' in the sense of joint working parties and consultative forums.

---

96 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 14.

97 *Evidence,* p. 83.

98 *Submission,* p. 128.

2.128 Some commentators envisage for Australia a structured model based on the National Infrastructure Protection Center's Infragard in the USA, whose secure website provides members with information about cyberintrusions and appropriate protections; or the Internet Fraud Complaint Center, a joint initiative of the FBI and the National White Collar Crime Center, to which crimes can be reported via a secure web page for investigation and referral to the appropriate law enforcement body. More integrated public-private cooperative ventures are being developed in the United States, including the recent formation of an IT Information Sharing and Analysis Centre. Government agencies and 19 technology vendors, including Cisco Systems, IBM, Hewlett-Packard and Microsoft, are said to have formed an alliance in order to set up a secure mechanism that they can use to exchange information about security vulnerabilites such as viruses and other potential threats to corporate and govenment computer networks.[99]

2.129 'Partnerships' involving the employment on contract of private sector experts by public sector agencies have in fact been underway for some time. Mr Gordon Williamson, Director of AFP Technical Operations, told the Committee that when a very high level of technical expertise was required, the AFP contracted it in from those at the cutting edge, as no agency could justify having it 'on tap' the whole time. He assured the Committee that the AFP had not been in the position of being unable to resolve an investigation because it lacked the necessary expertise:

> All the way along we have either had internally, or through relationships with our partner agencies *or other private industry sectors,* the right level of expertise to bring to bear on the job at the time.[100] [emphasis added]

2.130 The Committee was told of similar practices in a number of agencies. ASIC outsourced its computer forensic requirements to the AFP or to the large accounting firms.[101] AUSTRAC director Elizabeth Montano indicated that her agency also contracted in the computing expertise her agency needed, with contractors being paid market rates; however the agency also maintained sufficient in-house expertise to ensure that it was not being 'conned'.[102] CrimTrac representative Mr Kim Terrell described the IT industry as being very open and flexible in terms of the relationships it would enter into with the public sector and his aim for CrimTrac would be one of strategic partnerships with industry.[103]

2.131 While contracting in IT expertise was the pragmatic choice of many law enforcement agencies, it nevertheless raises security concerns. Mr Geoff Gray of the Commonwealth DPP's Office voiced the concerns of many when he stated:

---

99 Etter, B., 'Computer Crime', Paper presented at the 4th National Outlook Symposium on Crime in Australia, convened by the Australian Institute of Criminology, Canberra, 2001, p. 12.

100 *Evidence,* p. 146.

101 *Evidence,* p. 160.

102 ibid., p. 43.

103 ibid.

> there are great limits to the extent to which you can bring in those private sector skills. From my point of view, I would much prefer to see [computer forensic skills] remain within the AFP. People speak in glowing terms about contracts, but I just do not see how you can prevent leakage of confidential information. It is very much a second-best option, in my opinion.[104]

2.132 An even more fundamental question is whether there are sufficient suitably qualified people in either the public or private sectors to meet law enforcement's IT needs. Mr Rob Durie, Executive Director of the Australian Information Industry Association, told the Committee that there was an overall shortage of about 30,000 persons in the general IT field, let alone in highly specialised areas, and that present initiatives to provide extra places at universities were impeded by the lack of teachers and in any event would show no results for five years or more.[105] He reinforced the view that government-industry partnerships were the only realistic option.

2.133 The Committee received a great deal of evidence of the existence of a number of consultative forums and working groups, including the Law Enforcement Advisory Council (LEAC), the newly formed law enforcement taskforce chaired by the IIA[106] and the National Information Infrastructure Consultative Industry Forum.[107]

2.134 The e-crime strategy from the Police Commissioners' Conference particularly stresses the need for a cooperative relationship between law enforcement, the industries providing the networking and IT services, and the industries actually using the services.[108]

2.135 In relation specifically to e-commerce, AFP Commissioner Mick Keelty stressed the two-way nature of private sector partnerships with law enforcement. He noted that the private sector was producing or using technology for commercial reasons and hence it should be prepared to invest in its protection. He indicated that the general run of calls for assistance that the AFP received were largely from businesses complaining that their website had been hacked into, because they had inadequate or no security in place. He noted that the private sector response to proposed police-initiated security information forums had been 'pitiful'.[109]

2.136 Specific-issue working partnerships to deal with matters such as identity fraud appear to have been more successful. The NCA's Swordfish Task Force has established a Joint Agency Forum in NSW which has recognised the need, inter alia, to work with the private sector to encourage and assist in developing identity-checking

---

104 ibid.

105 ibid., pp. 69-70.

106 AGEC, *Submissions,* p. 253.

107 AIIA, *Evidence,* p. 77.

108 Police Commissioners' Conference, *Electronic Crime Strategy,* March 2001.

109 *Evidence,* p. 148.

strategies and to progress MOUs between law enforcement and regulatory agencies with respect to sharing identity data.[110]

2.137 The Committee notes that there is no one strategic relationship for all occasions, but those strategies which involve some form of public-private partnership will almost certainly be more effective. This partnership issue arises directly in the next section: in relation to the establishment of a national cyber-forensic unit.

A national cyber-forensics unit?

2.138 The capacity of law enforcement to keep up to speed with technological change was a recurring theme in evidence to the Committee. The RGEC report addressed the question of law enforcement's future computer forensic skills requirements and concluded:

> Many of the countermeasures to crime which exploits the characteristics of the Internet call for law enforcement and revenue agencies to use sophisticated tracing and other tools. They also call for these tools to be used by well trained specialists who retain their skills and maintain contact with industry. This would be a significant ongoing expense for government. To ensure such an investment is used effectively and as widely as is needed Australian governments should address the provision of a central computer and Internet forensic capability, available to all Commonwealth, State and Territory jurisdictions to support the investigation of computer and Internet-related crime.[111]

2.139 The Committee learnt that the AFP has electronic evidence teams of 12 and was 'upskilling' all its officers to a basic level of computing competence. AFP Commissioner Mick Keelty assured the Committee that 'at the moment we are meeting demand'[112] The NCA was doing much the same, maintaining an in-house capability for straightforward retrieval of electronically stored data,[113] but the question remains whether present approaches will suffice in the potentially more challenging technological future.

2.140 The NCA was firm in its view of the need for the establishment of a national law enforcement cyber-forensics facility for highly sophisticated data recovery. It acknowledged, however, that it was not practical or cost-effective for an organisation of the NCA's size to seek to develop such a capacity in-house. It would prefer to rely

---

110 *Submissions,* p.166.

111 RGEC, *Contributions to Electronic Commerce: what law enforcement and revenue agencies can do,* vol. 1, 1999, p. 119.

112 *Evidence,* p. 155.

113 NCA, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the management arrangements and adequacy of funding of the Australian Federal Police and the National Crime Authority,* February 2001, p. 23.

on a common national resource to provide the service.[114] The ABCI stressed that such a facility need not be a bricks and mortar establishment but that there was merit in considering a virtual capacity that used the specialist expertise in a number of organisations.[115]

2.141 The AFP confirmed the RGEC view that no agency could justify having on tap very high level technical expertise in every field. Faced with a request to investigate a high level attack on a banking system, the AFP now would contract in the expertise of those at the cutting edge.[116] As Mr Williamson explained, to maintain expertise you need continued work in a specific area, and the people who have that continued work are in the workplace or research centres. They are the people the AFP would seek to co-opt or contract as the need arose.[117] He added that the AFP would seek to maintain cutting edge expertise in-house in specific areas such as cryptography, which is always required.

2.142 The Committee notes that in the defence and security fields in Australia, the need for high-level computer capabilities has been recognised and acted upon. Following the Dudgeon and Cobb reports of 1997, a National Information Infrastructure Protection Secretariat was set up, and the National Computer Authority within the Defence Signals Directorate was expanded, as was the Defence Science and Technology Organisation's Advanced Computer Capabilities Branch. The latter was reported as employing over 40 scientists and professional software and hardware engineers in April 2000.[118] The computing needs of the law enforcement community should be reviewed in this context.

2.143 In the law enforcement field overseas, specialist cyber-forensic facilities have already been set up. In the USA, the National Infrastructure Protection Center was established in 1998 at the FBI; the DEA also has a Computer Forensics Program, now located in the Office of Forensic Sciences. The number of cases handled by the latter is reported as increasing at a rate of 30 per cent per year.[119]

2.144 In the Committee's view, the case for a cyber-forensic facility in Australian law enforcement seems persuasive. While a modest level of technological knowledge of data recovery or interception can be expected of law enforcement officers in all agencies, it would not be cost-effective, practical or even possible for all agencies to develop sophisticated in-house cyber-forensic capabilities. A shared facility is clearly the only realistic option. And while the Committee accepts the need for a close

---

114 NCA, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the management arrangements and adequacy of funding of the Australian Federal Police and the National Crime Authority,* February 2001, p. 23.

115 *Evidence,* p. 102.

116 *Evidence,* p. 147.

117 *Evidence,* p. 153.

118 NCA, *The NCA and Cybercrime: scoping paper,* June 2000, p. 29.

119 ibid., p. 32.

relationship with private sector expertise in this area, it believes there is a legitimate and very necessary role for a government facility to play.

2.145 The Committee therefore recommends that a national cyber-forensic facility be established. The Committee expresses no firm view on the location, size, precise format or funding arrangements for such a facility but notes that there are common police services which might serve as a model. In the planning of a cyber-forensic facility, particular attention will need to be paid to issues of recruitment and retention of relevant expertise.

Recommendation 9: That a national cyber-forensic facility be established.

2.146 In the longer term, a more ambitious broadly based cybercrime unit might be considered in Australia. Both the UK and the USA have moved in this direction. In the UK, the National Criminal Intelligence Service (NCIS), in its study of computer crime, recommended that the most successful method of policing serious computer misuse was via a single, dedicated national unit. Its role would be to investigate the more serious IT crimes, to act as a centre of excellence for cybercrime issues and to support local police forces in their investigations.[120] The recommendation was accepted, and it has been announced that some £50 million has been provided to build a national computer crime unit.[121]

2.147 Of the many developments in the cybercrime prevention field in the United States, one of the more interesting from the perspective of Australia has been the establishment by the FBI of a centralised capability for cybercrime investigations. The National Infrastructure Protection Center (NIPC) at FBI headquarters is overall program manager; 16 FBI field offices will have NIPC squads of seven or eight agents each, with nationwide, 193 agents dedicated to investigating NIPC matters.

2.148 It was recognised at the time of formation of the NIPC in 1998 that it could not accomplish its mission to 'detect, deter, assess, warn of, respond to, and investigate intrusions and illegal acts that target or involve [US] critical infrastructures' without outside assistance. Hence the setting up of the NIPC Outreach strategic partnership program, involving all levels of government and various private sector organisations. A secure communications network, InfraGard, connects the partners. Other initiatives include the National Cybercrime Training Partnership, and the Computer Analysis Response Team, with 142 personnel specialising in the recovery of evidence from electronic media. The FBI has been reported as anticipating

120 NCIS, Project Trawler:Crime on the Information Highways, NCIS, London, 1999, p. 23, as cited in Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, p. 72.

121 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, p. 72.

that, with the likely increase in high-tech crime, the number of required computer forensic examinations will rise to 6000 this year.[122]

Electronic authentication

2.149 It is widely accepted that the success of e-commerce depends on a trusted, open authentication framework since, without authentication, nobody can be sure of who or what they are dealing with over the networks. Authentication in the context of e-commerce is the means of proving who you are.

2.150 For commercial purposes, more complete authentication associating an individual's public key with other identification characteristics has been sought and possibly found in the form of digital certificates, issued by a trusted third party to identify the certificate holder. There has been a growth industry, particularly in the United States, in companies setting up as issuers of digital certificates. In Australia, the Commonwealth Government saw the need for a strategy to control the issue and management of digital certificates, for the secure delivery of Government services online as well as to encourage the uptake of e-commerce in the private sector. In October 1997 the then Office of Government Information Technology established Project Gatekeeper to develop a national framework for the authentication of users of electronic online services, consistent with the OECD Guidelines on Cryptography Policy. To date, the Australian Taxation Office, Baltimore Certificates Australia Pty Ltd and Health eSignature Authority have achieved full Gatekeeper accreditation; eSign Australia Ltd has achieved entry level accreditation and 17 other organisations are seeking accreditation to issue Australian Business Number Digital Signature Certificates (ABN-DSC).[123]

2.151 The private sector has been active in this area, with Australia's four major banks collaborating on Project Angus to issue digital certificates later this year to business customers; those certificates will exist in the global Identrus electronic trust and payments scheme but will also be recognised as ABN-DSC digital certificates and will be accepted by Commonwealth agencies.

2.152 To ensure national uniformity in this regard, the States and Territories agreed in November 2000 to the Gatekeeper strategy and to adopt the ABN-DSC initiative. A Gatekeeper Policy Advisory Committee has also been established. The end result should be that government agencies will be able to chose from a panel of service providers whose products and methods of delivery have been evaluated and accredited to meet appropriate standards of integrity and trust.

---

122 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, pp. 78-81.

123 www.govonline.gov.au/publickey/abn-dsc-angus.htm, visited 16 July 2001.

Regulation of high-tech tools?

2.153 Law enforcement agencies and others have occasionally voiced the opinion that the way to prevent misuse of advanced technological tools is to place restrictions on their sale to the public. In particular, software permitting the generation of false credit card numbers, or software providing high-level encryption, have been suggested as candidates for such treatment. Until quite recently, strong cryptography was the monopoly of defence establishments, yet now it has been democratised to the point that anyone can download it free from the web, although the Committee was told that the export of certain cryptographic products was still banned in the United States.[124]

2.154 Not surprisingly, industry groups were in favour of the free flowering of new technology, unimpeded by government intervention. The Australian Information Industry Association, for example, told the Committee:

> Industry should be permitted to develop, invest, innovate and market new products and services, the viability of which will be determined by market demand. New technology offences cannot be addressed by restricting access to the *technology*. Rather, it is the *use* to which they may be put that may lead to an offence being committed. Where necessary, potentially "dangerous" products, such as high level encryption, should be licenced rather than banned.[125]

2.155 In evidence to the Committee, Mr Marshall Irwin, Member of the NCA, suggested that 'trying to stop encryption is probably like King Canute trying to hold the tide back'[126] and that what law enforcement needed was the ability, in appropriate circumstances, to be able to go behind the encryption and to intercept and decode email messages.

2.156 Despite a superficial attraction to regulating access to technological tools which have a capacity to thwart law enforcement, the Committee recognises that, if it exists, the Brendan Abbotts of the criminal fraternity will gain access. Law enforcement simply has to find other ways to handle the situation.

Conclusions

2.157 Through its willingness to adopt new technology, Australia is well positioned to benefit from e-commerce. While certain characteristics of e-commerce, such as its global spread, its accessibility, its immediacy and use of cryptography, lend themselves to potential exploitation by money launderers, there is little evidence to date that it is being so exploited. A long list of traditional offences, including identity theft and fraud, have been facilitated by advances in mobile telephony, the Internet

---

124 *Evidence,* p. 65.

125 *Submissions,* p. 73.

126 *Evidence,* p. 21.

and encryption; and it is these developments, more than e-commerce per se, that have the potential to assist money launderers.

2.158 It seems to the Committee that lax security of computer systems and human negligence (or lack of integrity) are the chief culprits in much e-crime. The answer lies, not so much in law enforcement, but in target hardening. The technology is there, and is improving all the time and decreasing in cost, to thwart illegal access and to some extent at least to lessen the chances of system compromises from within.

2.159 From the evidence provided to it, the Committee believes that the NCA and its partner agencies are well aware of the potential law enforcement risks posed by e-commerce and are developing strategies or have strategies already in place to counter them. It is now a question of continuous monitoring of new technological and payment developments, and of continuous reassessment of law enforcement responses, supplemented by upgrading of officers' skills and by the establishment of a specialist cyber-forensic facility.

2.160 To meet the jurisdictional challenges of both e-commerce and money laundering, continued international negotiations are required to harmonise definitions of e-crime and search and seizure provisions, to synchronise law enforcement mechanisms and to extend and improve extradition and mutual assistance treaties. These matters are addressed in the following Chapter.

CHAPTER 3

THE ADEQUACY OF INTERNATIONAL LAW ENFORCEMENT COOPERATION

Introduction

3.1 With the increasingly global nature of crime, assisted by developments in transportation and communications systems, especially the Internet, it is critical that Australia is fully engaged in global law enforcement processes.

3.2 Such international cooperation will extend to working with countries whose legal systems, cultures and philosophies vary greatly from our own. The challenges in harmonising international law enforcement approaches are self-evidently considerable. A simple example relates to capital punishment. Australia does not support the death penalty. It generally refuses to provide mutual assistance to a requesting country in a criminal matter where the person might be subjected to the death penalty if found guilty, and will not extradite such persons. Given that some of our closest South East Asian neighbours impose capital punishment for drug-related offences and those countries are often the source of drugs trafficked into Australia, from whom Australia would wish cooperation in its law enforcement efforts, the issue highlights the potential for difficulties for the international community in readily coming to grips with problems on a global scale.

3.3 In this Chapter, the activities of some of the key multilateral organisations are described and some noteworthy developments highlighted. The Committee is naturally keen to draw lessons from these international deliberations about the adequacy of Australia's approaches to the challenges identified and to assess the appropriateness of Australia's role in the international debates.

The international forums - a brief outline

United Nations

3.4 The United Nations (UN) is the principal and most longstanding vehicle for international cooperation. It has been specifically addressing the issue of crime involving computer and telecommunications technologies actively since 1990. The Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders in that year recommended a series of measures relating to the modernisation of domestic offences, investigative procedures, rules of evidence, forfeiture, mutual legal assistance, the improvement of computer security and the better education of the public and training of officials.[1] And, as recommended by the Eighth Congress, a

1 *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, 1990, p. 6.

manual on the prevention and control of computer-related crime was compiled and published in 1994.

3.5 At the Tenth Congress, held in Vienna in April 2000, a Workshop on Crimes Related to the Computer Network was held which addressed in four panel discussions the following topics: the criminology of computer-related crime; problems associated with search and seizure on computer networks; problems associated with the tracing of communications on computer networks; and the relationships between law enforcement agencies and the computer and Internet industries. The Workshop made several recommendations, including calls for greater cooperation between governments and industry and improved international cooperation in tracing offenders.[2]

3.6 The General Assembly, in its resolution 55/59 of 4 December 2000, endorsed the Vienna Declaration on Crime and Justice, committed member states to work towards enhancing their ability to prevent, investigate and prosecute computer-related crime. Resolution 55/63 noted the value, inter alia, of eliminating safe havens for offenders, law enforcement cooperation on international cases, training and equipping of personnel, raising public awareness, and taking into account the need to protect individual freedoms and privacy while preserving the capacity of governments to fight criminal misuse of information technologies.[3]

3.7 The UN also in 2000 adopted a wide-ranging Convention against Transnational Organized Crime and two Protocols thereto, applying only to serious crimes involving organised criminal groups and elements of transnationality. Further workshops have continued to be held on the Convention. For example, a workshop held in Palermo in December 2000 noted that, with the proliferation of technologies on which crime relied, there were concerns about the danger of developing regulations prematurely. It further noted the potential for technological security developments.

3.8 In an earlier development, the United Nations Commission on International Trade Law (UNCITRAL) had developed a Model Law on Electronic Commerce, an international legislative template intended to harmonise domestic legal approaches to e-commerce. According to the submission of the Attorney-General's portfolio, Australia's *Electronic Transactions Act 1999* has adopted the Model Law's approach, structure and key concepts but has adapted it to suit Australian legal traditions and the policy aims of the Australian government.[4] An UNCITRAL Working Group on Electronic Commerce, in whose meetings representatives of the Attorney-General's Department have participated, is developing uniform rules for electronic signatures to

---

2 United Nations Economic and Social Council, Commission on Crime Prevention and Criminal Justice, *Conclusions of the Study on effective measures to prevent and control high-technology and computer-related crime,* Vienna, 2001, p. 6.

3 ibid., p. 7.

4 *Submissions,* pp. 216-217.

provide internationally recognised legislative guidance to countries considering legislation on this topic.[5]

Organisation for Economic Cooperation and Development

3.9 The Organisation for Economic Cooperation and Development (OECD), whose membership consists of 29 technologically advanced countries, including Australia, has taken a leading role in identifying the social and legal implications of new technology. As early as 1969 it created a Data Bank Panel to explore issues related to transborder data flows; which it followed with 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Although non-mandatory, the guidelines were developed to be minimum standards which could be adopted into domestic law by member states and have proved to be highly influential.[6]

3.10 Further non-mandatory guidelines followed. *Guidelines for the Security of Information Systems*, released in September 1992, were significant for their recognition of proportionality - they emphasised that, in determining security measures, the risks to be avoided should be balanced against the cost of the security measures. March 1997 saw the release of *Guidelines for Cryptography Policy* which reasserted the fundamental right of individuals to privacy while also permitting lawful access to plaintext or cryptographic keys of encrypted data. Finally, in December 1999, *Guidelines for Consumer Protection in the Context of Electronic Commerce*, were published which contained the overarching principle that consumers should be afforded no less protection in e-commerce than that afforded in other forms of commerce.

3.11 Australia is an active participant in the OECD's work on e-commerce, including privacy safeguards, consumer protection and authentication.[7] Officers of the Attorney-General's Department have chaired the OECD Working Party on Information Security and Privacy and the OECD Electronic Authentication Steering Group.[8]

Council of Europe

3.12 The Council of Europe (COE) is an intergovernmental organisation formed in 1949 by West European countries. Forty-one European nations are now members. As early as September 1995 it approved a recommendation that:

> Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under

---

5 Attorney-General's Department, *Annual Report 1999-2000,* p. 73.

6 Thomas D. and Loader B.D., eds, *Cybercrime: Law enforcement, security and surveillance in the information age,* Routledge, London, 2000, p. 163.

7 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* ACPR, Payneham SA, 2000, p. 9.

8 Attorney-General's Department, *Annual Report 1999-2000,* p. 70.

> their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.
>
> Specific obligations should be imposed on operators of public and private networks that offer telecommunications services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities.
>
> Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offences, without affecting its legitimate use more than is strictly necessary.[9]

3.13 A working group on cybercrime was created by the Council in 1997, which released its first draft convention on 27 April 2000. Several revisions later, the draft was presented to the European Committee on Crime Problems in June 2001 and is scheduled to go to the Committee of Ministers for adoption in September of this year. When completed, it will be open to signature by non-European nations some of which, like the United States, had contributed to the drafting process. The then Minister for Justice and Customs, Senator the Hon. Amanda Vanstone, informed the Committee in January 2001 that, while Australia had not been involved in the drafting of the COE convention, the Attorney-General's Department had been monitoring its development.[10]

3.14 The NCA submitted that the draft convention will be the first international treaty to address criminal law and procedural aspects of various types of offending behaviour directed against computer systems, networks and data.[11] Amongst other things, the convention seeks to create consistency amongst signatory states on the nature and form of legislation criminalising cybercrime, search and seizure of computer data, interception, and to provide mechanisms for mutual legal assistance amongst signatory states.

3.15 Specifically, the convention requires that signatory countries adopt laws requiring government access to encrypted information, criminalising the possession of common security tools and altering wiretapping laws. It is understood that only Malaysia and Singapore have existing laws requiring individuals to release encryption keys and decrypted data to government officials.

---

9 COE, *Recommendation of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information,* 1995 [www.privacyinternational.org/issues/cybercrime]

10 *Submissions*, p. 245.

11 ibid., p. 169.

3.16 The Federal Government has recently introduced the Cybercrime Bill 2001 to legislate for new computer offences which was based on the January 2001 Model Criminal Code *Damage and Computer Offences Report* and took into account the draft COE convention.[12] That Bill is currently the subject of inquiry by the Senate Legal and Constitutional Legislation Committee. In his Second Reading Speech on the Bill, the Attorney-General, the Hon. Daryl Williams MP, stated:

> Updated laws are vital if authorities are to effectively detect, investigate and prosecute cybercrime activities. The proposed new computer offences and investigation powers in the [Bill] are a significant development in the fight against these activities and will place Australia at the forefront of international efforts to address the issue of cybercrime.[13]

In relation specifically to the draft COE provision on government access to encrypted information, the Bill provides that a magistrate would be able to order a person with knowledge of a computer system to provide such information or assistance as is necessary and reasonable to enable the governmental officer to access, copy or print data.

European Union

3.17 The European Union (EU) has already taken a number of steps to promote electronic commerce and the use of electronic signatures, and to enhance the security of transactions, following the European Commission's 1998 report to the EU Council on computer-related crime. In 2000, the Council adopted a comprehensive *e*Europe Action Plan which highlights the importance of network security and the fight against cybercrime. In a January 2001 Communication from the European Commission to the Council, several proposals for action were advanced, including the creation of specialist computer crime police units in the 15 member countries, support for appropriate technical training for law enforcement and encouragement of information security action.

3.18 The Commission is currently engaged in developing proposals to harmonise high-tech crime offences among member states and to go further than the draft Council of Europe Convention on Cyber-Crime by ensuring that serious cases of hacking and denial of service attacks are punishable by a minimum penalty in all member states.[14]

3.19 The Commission also indicated its intention to set up an EU Forum in which law enforcement agencies, ISPs, telecommunications operators, consumer representatives, civil liberties organisations and other interested parties could jointly

---

12 House of Representatives, *Hansard,* 27 June 2001, p. 27082.

13 ibid., p. 27081.

14 European Commission, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime,* Brussels, 2001, p. 15.

discuss ways to raise public awareness of Internet crime, best-practice security measures and procedures to combat computer-related crime.[15]

Group of 8

3.20 The Group of 8 (G8) comprises the eight leading industrialised countries of the world, namely Britain, Canada, France, Germany, Italy, Japan, Russia and the USA. It was formed as the G7 (without Russia) at an economic summit in France in 1975. A G8 Subgroup on Hi-Tech Crime was formed in 1997. Its activities to date have included the establishment of a network of emergency contacts, the hosting of a computer crime conference for law enforcement personnel, the review of G8 legal systems relating to high-tech crime and examination of the issue of the location and identification of criminals who use networked telecommunications.

3.21 In 1997, the G8 Justice and Interior Ministers issued a *Statement of Principles* concerning electronic crime. These principles included statements against safe havens for criminals, coordination of investigations, training and equipment of law enforcement personnel, protection of confidentiality, development of forensic standards for retrieving and authenticating electronic data. It also suggested that work in this area should be coordinated with the work of other relevant international forums to ensure against duplication of effort.[16]

3.22 In October 1999 the G8 formulated principles on *Transborder Access to Stored Computer Data*, to be implemented through treaties and national legislation. The principles are based on the need for states to establish legal mechanisms which enable them to rapidly access and preserve computer data, on request by another state. Further work is being undertaken on the preservation and disclosure of traffic data, tracing networked communications across national borders, and developing compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.[17]

3.23 A G8 conference in Paris in May 2000 considered particularly how governments and industry should interact to counter cybercrime without discouraging the growth of e-commerce. Its outcomes included a recognition of the indispensable nature of international cooperation and the need to ensure that there are no safe havens for cybercriminals, a proposal to require ISPs to store a year's worth of information about the websites visited by subscribers and the email messages they sent, and the

15 European Commission, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime,* Brussels, 2001, pp. 2-3.

16 See Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* Payneham SA, ACPR, 2000, p. 66.

17 Attorney-General's portfolio, *Submissions,* p. 227.

establishment of a global, around the clock system of cybercrime contacts.[18] The AFP houses Australia's 24-hour cybercrime response centre.

Financial Action Task Force on Money Laundering

3.24 The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering, defined as the processing of criminal proceeds in order to disguise their illegal origin. The aim is to prevent such proceeds from being used in future criminal activity and from affecting legitimate economic activity.

3.25 It was established in 1989 by the G7 countries, with Australia being a founding member. In 1991 the G7 Council of Ministers appointed the then Chairman of the NCA, Mr Justice John Phillips, as FATF President, an honour that was extended to his successor, Mr Tom Sherman. The current membership comprises Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, China, Iceland, Ireland, Italy, Japan, Luxembourg, the Kingdom of the Netherlands, New Zealand, Norway, Portugal, Singapore, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States, plus two international organisations, the European Commission and the Gulf Cooperation Council.[19]

3.26 A major initiative of FATF, and one in which Australia played a major role, was the drafting of the *40 Recommendations*, which have become widely accepted internationally as world's best practice anti-money laundering policy guidelines. Those recommendations include:

- each country should criminalise money laundering;
- each country should confiscate proceeds of crime;
- financial institutions should identify customers, not keep anonymous accounts, and maintain identification records for at least five years after the account is closed;
- financial institutions should maintain transaction records for at least five years;
- financial institutions should develop programs against money laundering and should monitor and report on suspect transactions, particularly those involving countries which do not abide by the *40 Recommendations*;
- countries should monitor the physical cross-border transportation of cash and bearer negotiable instruments;

---

18 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* Payneham SA, ACPR, 2000, pp. 67-68.

19 AUSTRAC, *An Overview of Australia's Anti-money Laundering Strategy,* May 2000, p. 2.

- systems for reporting to a national central agency domestic and international currency transactions over a fixed amount should be set up; and
- there should be administrative cooperation, mutual assistance and extradition cooperation with other countries' appropriate authorities.[20]

3.27 Each member country's own conduct in upholding the *40 Recommendations* is subject to evaluation by FATF and self-assessment exercises by individual countries. Australia's anti-money laundering initiatives to date are outlined in Chapter 2. The 1996 FATF peer review of Australia's performance resulted in a glowing endorsement:

> Australia can pride itself on a well-balanced, comprehensive and in many ways exemplary system, and must be congratulated accordingly. It meets the objectives of the FATF Recommendations and is constantly reviewing the implementation of their anti-money laundering provisions, simultaneously looking well into the future.[21]

3.28 The inter-relationship of financial sectors and the cross-border activities of some criminals and money launderers led to the recognition that it was necessary to promote anti-money laundering activities in the region. As described below, an Asia-Pacific Group on Money Laundering (APG), affiliated with the FATF, was set up with a secretariat in the Sydney office of the NCA in 1997. Similar regional groups have been developed in other regions.

3.29 Since the end of 1998, the FATF has taken a lead in identifying those jurisdictions with rules and practices which impede the fight against money laundering. It devised 25 criteria against which jurisdictions could be assessed and, in a review published in June 2000 after relevant inspections, it named the following 15 countries or jurisdictions as non-cooperative or with serious systemic problems: Bahamas; Cayman Islands; Cook Islands; Dominica; Israel; Lebanon; Liechstenstein; Marshall Islands; Nauru; Niue; Panama; Philippines; Russia; St. Kitts and Nevis; and St. Vincent and the Grenadines. The issues of particular concern included lax customer identity requirements by financial institutions; difficulties in establishing the beneficial ownership of some legal entities; and bank secrecy provisions.[22]

3.30 The FATF offered assistance to help these jurisdictions mend their ways but also warned that, should they fail to make adequate progress in doing so, countermeasures would be applied. It further warned its members that 'financial institutions should give special attention to business relations and transactions with

---

20 FATF, *The Forty Recommendations,* OECD, Paris, (1990).

21 FATF, *Annual Report 1996-97,* 1997, p. 13.

22 FATF, *Review to Identify Non-Cooperative Countries or Territories: Increasing the Worldwide Effectiveness of Anti-Money Laundering Measures,* June 2000.

persons, including companies and financial institutions, from the "non-cooperative countries and territories".[23]

3.31 A second review has recently been completed. Six new jurisdictions have been identified as non-cooperating in the global fight against money laundering (Egypt, Guatamala, Hungary, Indonesia, Myanmar and Nigeria); four countries on the 2000 list have made sufficient progress to be removed from the list (Bahamas, Cayman Islands, Liechstenstein and Panama); progress has been noted in seven jurisdictions though they continue to be listed (Cook Islands, Dominica, Israel, Lebanon, Marshall Islands, Niue, and St Kitts and Nevis); and in three jurisdictions (Nauru, the Philippines and Russia), such inadequate progress has been made that unless significant anti-money laundering legislation is enacted before 30 September 2001, FATF recommends 'the application of further counter-measures which should be gradual, proportionate and flexible regarding their means'.[24] In short, this means that they are not to be black-balled from the international financial system just yet. It is hoped that the counter-measures will go some way to reducing the vulnerability of the international financial system and increase the world-wide effectiveness of anti-money laundering measures.

3.32 Typical of the problems which the FATF wants to counter is the practice of money-raising via the licensing in certain jurisdictions of offshore 'banks' which are poorly supervised and which operate with excessive secrecy provisions. Nauru was found to have about 400 such banks and the Cook Islands seven. Similarly the practice of registering international companies without adequate information about them - and the Cook Islands has some 1200 such companies - is frowned upon, because of the obvious assistance this offers money launderers.

Asia-Pacific Group on Money Laundering

3.33 The Asia-Pacific Group on Money Laundering (APG) was established in 1997. As indicated above, it is one of the regional anti-money laundering groups affiliated with the FATF, with a membership comprising 22 countries from South Asia, South East and East Asia and the South Pacific: Australia; Bangladesh; Chinese Taipei; Cook Islands; Fiji; Hong Kong; China; India; Japan; Macau; China; Malaysia; New Zealand; Niue; Pakistan; Republic of Indonesia; Republic of Korea; Republic of the Philippines; Samoa; Singapore; Sri Lanka; Thailand; USA and Vanuatu. The Sydney-based secretariat was initially funded by Australia as an Asian outreach strategy[25] although now all members of the group contribute.

3.34 The Group's fourth annual meeting was held in Kuala Lumpur, Malaysia, in May 2001. Other regular meetings look at money laundering typologies. The APG

---

23 ibid., p. 12.

24 FATF, *Review to Identify Non-Cooperative Countries or Territories: Increasing the Worldwide Effectiveness of Anti-Money Laundering Measures,* June 2001, p. 4.

25 AUSTRAC, *An Overview of Australia's Anti-Money Laundering Strategy,* May 2000, p. 8.

secretariat serves as a focal point for the coordination of anti-money laundering technical assistance and training in the region.

3.35 The presence of a number of the FATF-listed 'non-cooperative countries and territories' in the APG is clearly a challenge for the group as a whole.

Asia-Pacific Economic Cooperation

3.36 In response to the growing inter-dependence amongst Asia-Pacific economies, the Asia-Pacific Economic Cooperation (APEC) was established in 1989 to promote open trade and economic cooperation amongst its now 21 members. Ten working groups have been established, including one on telecommunications and an Electronic Authentication Task Group.

Council for Security Cooperation in the Asia Pacific

3.37 The Council for Security Cooperation in the Asia Pacific has been described as an unofficial think tank, supporting the ASEAN Regional Forum. Australia is a co-chair, along with the Philippines and Thailand. It supports the Asia-Pacific Working Group on Transnational Crime, in which Australia participates.[26]

Interpol

3.38 Interpol is the shortened title for the International Criminal Police Organization, headquartered in Lyon, France, and the successor to the first international police cooperative body which had been established in Vienna in 1923. It has 178 members worldwide and aims to ensure and promote the widest possible mutual assistance between all criminal police authorities, within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights.

3.39 Interpol's broad objective in relation to computer crime is to enhance law enforcement's international capacity to respond to information technology based crime. Its General Assembly recommended the establishment of five global regions; the first Asian Region (English speaking) Working Party was convened in Melbourne in February 1997. The European Working Party produced the *Interpol Computer Crime Manual*, which has been made available through the Australasian Centre for Policing Research to all Australian police agencies.[27] The AFP is Australia's central reference point for Interpol information exchange, including of computer crime messages. Interpol maintains a database on a secure website of images and operational information on counterfeit payment cards, available to all operational law enforcement agencies and the payment card industry; it is adding to its impressive cross-border art theft intelligence network with cybercrime information.

---

26 Attorney-General's portfolio, *Submissions,* p. 230.

27 Police Commissioners' Conference Electronic Crime Project Working Party, *The Virtual Horizon: Meeting the Law Enforcement Challenges,* Payneham, SA, ACPR, 2000, p. 64.

3.40 As noted in the Preface, the Committee in the 38th Parliament met with the then Secretary General of Interpol, Mr Raymond Kendall, in Canberra in December 1996. The cybercrime issue formed part of the discussion, with Mr Kendall making the observation that such issues were often addressed by the passage of national laws when essentially only an international approach can address international problems of this nature. He noted the signs of positive progress in international law enforcement, such as the adoption by the United Nations in Vienna in 1988 of the *Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, which laid the basis for a level of international cooperation on drug trafficking. He had stressed, however, that problems then arise with the practical implementation of such conventions when countries do not act promptly to adapt their national legislation to meet the requirements of the convention.[28]

World Customs Organization

3.41 The Customs Cooperation Council, renamed the World Customs Organization (WCO) in 1994, is an independent intergovernmental body with some 150 member governments worldwide. Its aim is to enhance the efficiency and effectiveness of Customs administrations. Key activities include the development of a law enforcement database, the Customs Enforcement Network, a secure website to provide constantly updated shared data to members. The concept is based on the premise that transnational crime is transborder crime and hence improved Customs communications and intelligence sharing can mean more effective action against transnational crime.[29]

3.42 The WCO also supports a Working Group on Transnational Organised Crime, in which the Australian Customs Service participates.

International Organization on Computer Evidence

3.43 Following the G8's recognition of the need for common computer evidence standards with respect to criminal activity that crosses international borders, the International Organization on Computer Evidence (IOCE) was set up, holding its first meeting in 1993, involving computer forensic experts from the G8 countries. Membership has now been extended to others. The AFP is Australia's representative on the IOCE board.[30]

3.44 IOCE is particularly active in developing standards relating to computer evidence, for ratification by G8 countries. It is also working on issues such as

---

28 See the Committee's February 1997 report entitled *Law Enforcement in Australia - An International Perspective* for a summary of the meeting with Mr Kendall. The transcript of the public hearing held with Mr Kendall on 5 December 1996 can be accessed through the Committee's webpage at http://www.aph.gov.au/nca.

29 Attorney-General's portfolio, *Submissions,* pp. 229-230.

30 Attorney-General's portfolio, *Submissions,* p. 231.

international accreditation and validation of tools, techniques and training in forensic computing.

Australia's participation in international forums

3.45 This above listing of international forums with elements of law enforcement cooperation, while impressive in terms of the sheer volume of activity, is almost certainly not exhaustive. With so much concurrent international activity, the Committee was interested to learn the extent to which Australian law enforcement authorities were involved and, accordingly, the extent to which Australia's concerns were being heard in the international arena.

3.46 The then Minister for Justice and Customs, Senator Amanda Vanstone, assured the Committee that officers posted overseas from the Department of Foreign Affairs and Trade (DFAT), where possible, attended relevant meetings and reported back to the department and law enforcement agencies.[31] The AFP also participates in a number of international forums on electronic crime and reports back to the Australasian Police Ministers' Council and the Heads of Commonwealth Law Enforcement Agencies.[32]

3.47 Given the tyranny of distance and the cost implications of attendance at such conferences, the Committee accepts that maximising the use of locally based DFAT staff is sensible. One obvious drawback, however, is that there must be doubts about the capacity for generalist DFAT officers to contribute meaningfully to technical discussions about law enforcement issues, and to forcefully press Australia's case, rather than to merely act as observers.

Australia's transnational law enforcement relationships

3.48 New technology crime ignores international borders and is becoming adept at exploiting differences in legal systems and gaps in international cooperation. Hence practical international cooperation is vital. Australia's law enforcement relationships with foreign countries are governed by two key pieces of legislation: the *Extradition Act 1988* and the *Mutual Assistance in Criminal Matters Act 1987.*

3.49 The Attorney-General's portfolio submission suggested that Australia's extradition regime had been modernised by the opening up of the kinds of extraditable offences that include computer crime and by the implementation of 'no evidence' extradition arrangements to overcome the problem of differing evidentiary laws between countries.[33]

3.50 The Mutual Assistance in Criminal Matters Act provides the legislative basis for Australia to enter into arrangements with other countries to request and grant

---

31 *Submissions*, p. 245.

32 ibid., pp.245-246.

33 *Submissions,* p. 225.

assistance in criminal matters. Bilateral mutual assistance treaties have been negotiated with a wide range of countries and from 1 March 1997 the Act applied 'passively' to all foreign countries - where appropriate, the Attorney-General can request or grant mutual assistance concerning a particular jurisdiction. The types of assistance covered by the Act include the taking of evidence, the production of documents, the issue of search warrants, the seizure of relevant things, and the freezing, seizure and forfeiture of proceeds of crime.

3.51 The Attorney-General's Department publishes statistics on both extradition and mutual assistance requests by and to Australia. In 1999-2000 Australia made six new extradition requests to other countries and 17 cases were carried forward; six requests were granted and one was refused. Twenty-two new extradition requests were made of Australia and 34 were carried over, in the same period; 13 were granted and 3 refused. Australia made 61 new mutual assistance requests in 1999-2000 and 41 cases were carried forward; of these, 61 were executed and one was refused. In the same period 149 mutual assistance requests were made to Australia and 66 cases carried forward; 122 requests were executed and none was refused.[34]

3.52 There has been a steady upward trend in the number of mutual assistance requests made of Australia over the last four years. In purely numerical terms, Australia 'gives' up to twice as much as it 'receives' though this may not necessarily reflect the amount of work involved. And the process can be exceedingly slow: Swiss authorities provided extensive materials for a particular Australian investigation, into conduct by former directors of Elders IXL Ltd, some nine years after the request was made.[35] This inquiry was one in which the NCA had played a prominent role.

3.53 The deficiencies of the current mutual assistance scheme were addressed in four of the seven submissions received from government/police service representatives of the States and the Northern Territory. The Queensland Minister for Police and Corrective Services, the Hon. Tom Barton, noted:

> Jurisdictional differences in what constitutes a crime inhibits international cooperation at an operational level. While overarching mutual assistance agreements may be in place between jurisdictions, these often require that the grounds on which assistance is sought be defined as a crime both in the requesting country and in the assisting jurisdiction.[36]

3.54 The Victorian Government submitted:

> The effectiveness of the traditional means of cooperation through Mutual Assistance applications is already compromised by administrative delays. The situation is aggravated by technology facilitated crime crossing borders instantaneously. The need to develop and maintain consistent legislation

34 Attorney-General's Department, *Annual Report 1999-2000,* p. 200.

35 ibid., p. 75.

36 *Submissions*, p. 92

> and efficient investigation protocols is becoming more urgent as the methodology used in the commission of crime continues to be influenced by the advent of new technology. [37]

3.55 Northern Territory Police Commissioner, Mr Brian Bates, described the traditional system for making mutual assistance requests as 'cumbersome and lengthy when dealing with electronic crime'[38] while the then Western Australian Police Minister, the Hon. Kevin Prince, conveyed the sentiments of the Computer Crime Investigation Unit in similar terms, that:

> bureaucratic procedures incorporated within the Commonwealth's *Mutual Assistance in Criminal Matters Act 1987* do not facilitate timely intervention in, and resolution of, such [computer crime] criminal matters.[39]

3.56 Mr Prince then gave a detailed account of attempts by his investigators to use alternative international mechanisms, such as Interpol and the International High Tech Crime Contact list, both accessed through the AFP. In one case, a complaint was received by the WA Police Service in November 1999 relating to an extortion attempt via email. Police immediately secured evidence and imaged hard drives. The email header information led to a source Internet Protocol registered to an UK ISP. The ISP complied with a request to preserve the relevant logs for evidentiary purposes. However, the local UK police were reluctant to assist until the request came through official channels. The request was made through formal channels, through the Bureau of Criminal Intelligence within the WA Police Service and Interpol. A short response, insufficient to base further action on, was received over six months later, effectively bringing the inquiry to a halt. Mr Prince noted a second case where no response had been received after three months.[40]

3.57 The frustration expressed at such delays by State/Territory government submitters is, quite clearly, understandable and the Committee notes that the onus is on the Commonwealth Government to seek to take appropriate action to address these concerns.

3.58 It appears that two major impediments exist in the mutual assistance field: limitations on the nature of the investigative assistance that can be offered; and the problems posed by the need for real-time assistance in electronic crime.

3.59 Firstly, Australian law enforcement officers cannot apply for a telecommunications interception or listening device warrant to support a foreign investigation (although if the conduct under investigation might be an offence against Australian law, police could instigate their own investigation). Only certain

---

37 *Submissions,* p. 141.

38 ibid., p. 46

39 ibid., p. 111.

40 ibid., pp. 111-112.

information may be passed to foreign investigators: AUSTRAC data[41] and telecommunications intercept material obtained for an existing Australian investigation.[42] The Attorney-General's portfolio has recognised the problem. It submitted that:

> Based on reciprocity the basic principle which could be considered is that, subject to appropriate controls and safeguards, an investigation tool which is available to support an Australian investigation should also be available to support a foreign investigation into a like offence, unless there is some reason to the contrary…Necessary refinements to the mutual assistance regime to accommodate such developments will be considered, as appropriate.[43]

3.60 Secondly, the instantaneous nature of cybercrime mandates the need for real-time investigation in many cases, so offenders can be caught while still connected electronically. Specifically addressing this issue is clearly the overwhelming demand of submitters to this inquiry.

3.61 As the Attorney-General's submission noted:

> In common with worldwide arrangements, Australia's current mutual assistance regime is geared to the type of investigation which takes place after an offence has been committed and in which the police are attempting to understand what took place after the event. However, this might not be the most effective way to fight e-crime. If investigators are required to wait until the offence is completed, the electronic trail will be cold, computer connections will have been discontinued and the data and the evidence lost.
>
> In a real-time investigation, police would seek to secure admissible evidence of criminal conduct. They would wait until a fresh crime is being committed and then undertake an investigation while the offender is still electronically connected and online so that the relevant messages could be traced back to their source and the offender could be detected red handed.[44]

3.62 Once again, it appears that the Council of Europe's Draft Convention on Cyber-Crime contains appropriate measures to address this problem. Beyond calling for parties to provide traditional forms of mutual assistance and extradition, it also proposes the setting up of a network of 24 hours a day, seven days a week national contact points to speed up international investigations. The NCA's submission drew particular attention to this proposal and expressed its in principle endorsement of the cooperative approach required by the draft convention.[45]

---

41 This is permitted under the *Financial Transaction Reports Act,* s.37A and subsection 27(3A).

42 Permitted under the *Telecommunications (Interception) Act 1979,* paragraph 5B(h).

43 *Submissions,* p. 229.

44 *Submission*s, pp. 228-229

45 ibid., pp. 169-170.

Conclusions

3.63 The Committee has found there to be no shortage of international effort in addressing the need for international law enforcement cooperation to meet the challenges of new technology. That is unquestionably a positive development and one that the Committee welcomes. Equally, there appears to be a fair degree of duplication and little overall coordination, a point noted by the United Nations Commission on Crime Prevention and Criminal Justice.[46] It is worth noting, however, that all discussion at these forums is making a contribution to informing deliberations in Australia, even if there is an element of repetition in its content.

3.64 Australia's participation in these international forums is clearly patchy but - as noted by the Federal Privacy Commissioner with somewhat brutal candour - as a relatively small player on the global scene, Australia may end up at the end of the day having to be a policy taker in this area in order to avoid the adverse consequences of international odium.[47] However, given Australia's respected role in forums such as FATF and its leadership role in taking action to address problems highlighted through international forums, such as in relation to the fight against money laundering, the Committee is confident that its contributions to international deliberations carry sufficient weight to ensure that Australia's interests will at least be given due consideration in the decision-making process.

3.65 In introducing the Cybercrime Bill 2001, the Government has stated that it has taken the Council of Europe's deliberations into account. Given that the intention of the Council's Draft Convention on Cyber-Crime is 'to harmonise national legislation in this field, facilitate investigations and allow efficient levels of cooperation between authorities of different States', and given that such non-European countries as Canada, Japan, South Africa and the United States are active participants in its processes, it appears to the Committee that the Government has made a sensible and pragmatic choice.

3.66 The Committee recognises, however, that the convention is only in draft form and it has not yet been signed. The Committee also notes that some industry and privacy groups in Australia have concerns about aspects of the draft convention which remain to be addressed. Whether the Government's legislation will indeed place Australia 'at the forefront of international efforts to address the issue of cybercrime', as claimed by the Attorney-General, or whether it will prove to be a case of 'premature regulation',[48] will only become clear with the benefit of practical experience.

---

46 United Nations Economic and Social Council, Commission on Crime Prevention and Criminal Justice, *Conclusions of the Study of effective measures to prevent and control high-technology and computer-related crime: Report of the Secretary-General,* Tenth session, item 4, Vienna, May 2001, pp. 16-17.

47 *Submissions*, p. 260.

48 In *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities* (reproduced in *Submissions*, p. 14) Grabosky and Smith wrote: Current wisdom, in [e-commerce] as in other areas of telecommunications-related crime, is inclined against what might be referred to as premature regulation. Untimely regulatory intervention runs the risk of stifling innovation and product development.

3.67 From the NCA's viewpoint, given that most of its activities have an international dimension, the need for Australia to be fully engaged in the process of international cooperation, whether in the form of mutual assistance, extradition arrangements and purposeful international treaties, has never been greater. Meaningful international cooperation is also dependent, however, on individual nations addressing within their own jurisdictions any unwarranted legal limitations on the forms of assistance that they can offer to their international law enforcement partners. The Committee urges the Government to give priority attention to identifying any such problems, some of which have been described above, and to seek to introduce appropriate remedial measures.

APPENDIX 1

SUBMISSIONS

1	Australian Institute of Criminology
2	Confidential
3	Tasmanian Minister for Police and Public Safety
4	Tasmania Police
5	Northern Territory Police
6	Australian Securities and Investments Commission
7	Victoria Police
8 & 8a	Australian Federal Police
9	ACT Attorney-General
10	Australian Information Industry Association
11	The Distillery Pty Ltd
12	Privacy New South Wales
13	Queensland Minister for Police and Corrective Services
14	New South Wales Director of Public Prosecutions
15	Western Australian Minister for Police and Emergency Services
16	New South Wales Minister for Police
17	Australian Taxation Office

18	Commonwealth Ombudsman
19	Queensland Crime Commission
20	Australian Bureau of Criminal Intelligence
21	Victorian Government
22 & 22a	National Crime Authority
23 & 23a	Commonwealth Attorney-General's portfolio
24	Confidential
25	Electronic Frontiers Australia
26	Action Group into the Law Enforcement Implications of Electronic Commerce
27	Federal Privacy Commissioner
28	The Australian Privacy Charter Council

APPENDIX 2

WITNESSES AT PUBLIC HEARINGS

6 November 2000, CANBERRA

National Crime Authority:
Mr Marshall Irwin, Member
Mr Adrien Whiddett, General Manager, Operations

4 December 2000, CANBERRA

Attorney General's Department:
Mr Karl Alderson, Acting Assistant Secretary, Criminal Law Branch
Ms Sandra Ellims, Assistant Secretary, Law Enforcement Branch, Criminal Justice Division
Mr Chris Hodges, Principal Legal Officer, International Branch, Criminal Justice Division
Mr Peter Treyde, Principal Legal Officer, Information Security Law Division

Australian Customs Service:
Mrs Marion Grant, National Manager, Border Operations Branch
Mr Peter Naylor, National Manager Investigations

Office of the Director of Public Prosecutions:
Mr Geoffrey Gray, Senior Assistant Director

Australian Transaction Reports and Analysis Centre:
Ms Elizabeth Montano, Director

CrimTrac Agency:
Mr Kim Terrell, Acting Chief Executive Officer

Australian Federal Police:
Mr Mark Walters, Acting Director, Technical Operations

2 March 2001, CANBERRA

Commonwealth Ombudsman:
Mr Frederick Bluck, Director, Policy
Mr Philip Moss, Senior Assistant Ombudsman

Australian Information Industry Association:
Mr Robert Durie, Executive Director
Ms Bridget Larsen, Legal and e-Policy Manager
Mr Murray Rankin, Representative

Australian Bureau of Criminal Intelligence:
Mr Peter Edwards, Deputy Director
Mr Neville Hewett, Manager, Information Services
Mr Mark Holmes, Manager, National Intelligence Association
Dr Grant Wardlaw, Director

Australian Institute of Criminology:
Dr Peter Grabosky, Deputy Director
Dr George Urbas, Research Analyst, Sophisticated Crime Program

26 March 2001, CANBERRA

Victoria Police:
Detective Inspector Stephen Berriman, Officer in Charge, Technical Support Unit
Inspector Stephen Leane, Manager, Legislative Review and Proposals Unit

Privacy New South Wales:
Dr John Gaudin, Legal and Policy Officer

Internet Industry Association:
Ms Mary-Jane Salier, General Counsel, UUNET and OzEmail Internet

2 April 2001, CANBERRA

Office of the Director of Public Prosecutions, New South Wales:
Mr Nicholas Cowdery QC, Director of Public Prosecutions

Australian Federal Police:
Ms Audrey Fagan, Acting Deputy Commissioner
Mr Michael Keelty, Acting Commissioner
Mr Gordon Williamson, Director, Technical Operations

Australian Securities and Investments Commission:
Mr Keith Inman, Director, Electronic Enforcement
Ms Nicole Pyner, Senior Lawyer, Enforcement Coordination