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.