Government Response to the Report of the Parliamentary Joint Committee on the National Crime Authority

The Law Enforcement Implications of New Technology

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.

Response: Accept.

As part of the ongoing review of the Telecommunications (Interception) Act 1979, the Government monitors the range of offences prescribed under sections 5(1) and 5D of the Telecommunications (Interception) Act 1979 and considers amendments, as appropriate, in light of technological developments.

The Telecommunications Interception Legislation Amendment Act 2002 was passed by Parliament on 27 June 2002. The Act amended the Telecommunications (Interception) Act 1979 to include child pornography, serious arson and terrorism offences within the list of serious offences in relation to which a telecommunications interception warrant can be sought.

Telecommunications services such as the Internet and e-mail are increasingly employed in perpetrating child pornography related offences. In some cases relevant offences are committed exclusively via electronic means. The amendment is intended to strengthen the Telecommunications (Interception) Act 1979 by ensuring the availability of telecommunications interception as an investigative tool in connection with the investigation of child pornography related offences. Consistent with the existing serious offence threshold provided in the Telecommunications (Interception) Act 1979, a warrant authorising telecommunications interception can only be sought in relation to child pornography related offences where the relevant offence is punishable by seven years or more imprisonment.

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

Response: Noted.

Policy considerations relating to national security are different to those relating to law enforcement. It is not appropriate, therefore, to automatically extend telecommunications interception related foreign intelligence warrants to law enforcement agencies.

There may be circumstances where it would be appropriate, on a case by case basis, to facilitate foreign intelligence gathering by law enforcement agencies. The Government is considering the extent to which intelligence agencies may assist law enforcement agencies in the collection of intelligence relevant to the investigation of serious and organised crime.

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

Response: Reject

The Telecommunications (Interception) Act 1979 reflects a carefully achieved balance between the protection of personal privacy in communications and the public interest in law enforcement and security. That balance would be difficult to ensure if powers were devolved to States and Territories on the basis of `broad-based mirror legislation'.

Further, the devolution of powers to the States and Territories could lead to an environment of greater regulatory and administrative complexity for carriers and carriage service providers. This could have adverse business consequences for carriers and carriage service providers and could also reduce the efficiency and effectiveness of their cooperation with law enforcement and security agencies.

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.

Response: Accept

Internet service providers (ISPs) are regulated under the Telecommunications Act 1997 as they fall within the definition of `carriage service providers'. The Government is of the view that under this regime an appropriate and realistic level of co-operation has been achieved between ISPs and law enforcement agencies.

The continued co-operation between law enforcement agencies and ISPs is an issue which is addressed in forums such as the Law Enforcement Advisory Committee which is chaired by the Australian Communications Authority.

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

Response: Accept

The Telecommunications (Interception) Act 1979 is drafted to be technology neutral. The Government is engaged in an ongoing review of the operation of the Telecommunications (Interception) Act 1979 to continuously monitor and consider the impact of emerging technologies on the operation of the Act. This review is done via an extensive consultative network with relevant stakeholders. For example, the Interception Consultative Committee (ICC) is a forum constituted by the Attorney-General's Department and intercepting agencies including the Australian Crime Commission and the Australian Federal Police. The ICC meets quarterly and is a useful forum to deal with both technical and legal policy issues arising from interception activities.

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.

Response: Accept.

The Government is actively considering the issue of comprehensive electronic surveillance legislation. At the Leaders' Summit on Terrorism and Multi-Jurisdictional Crime held on 5 April 2002, the Commonwealth and the States and Territories agreed to legislate through model laws for all jurisdictions for the use of electronic surveillance devices. Appropriate safeguards for the protection of personal privacy will be examined in the development of any legislative regime to deal with electronic surveillance.

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.

Response: Accept in part.

Some legislative restrictions on the capacity of law enforcement to exchange intelligence and operational information exist for good reason. Such restrictions are the result of balancing individuals' interests in maintaining their privacy with the public interest in law enforcement. However, the Government recognises the need to ensure that there are no unnecessary restrictions and to monitor the operation of legislation to ensure that, where a demonstrated and legitimate need for the exchange of intelligence and operational information exists, such exchanges are not prevented.

The Attorney-General's Department will consult with Commonwealth law enforcement agencies to identify Commonwealth legislative restrictions that may “inadvertently and unnecessarily restrict” the capacity of law enforcement agencies to exchange intelligence and operational information. The Department, in consultation with Commonwealth law enforcement agencies and the Federal Privacy Commissioner will then conduct a review of the legislative provisions that have been identified. The review will consider whether each provision achieves the appropriate balance between the privacy of the individual and the efficient conduct of law enforcement activities. The terms of reference of the review will be agreed between the Attorney-General, Commonwealth law enforcement agencies and the Federal Privacy Commissioner.

The impact of State and Territory laws that regulate the activities of law enforcement agencies is a matter best addressed by State and Territory Governments.

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.

Response: Noted.

The extension of the Commonwealth Ombudsman's jurisdiction over the use of electronic surveillance devices will be considered as part of the Government's work to implement the agreement of the Leaders' Summit on Terrorism and Multi-Jurisdictional Crime to develop legislation regulating electronic surveillance.

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

Response: Accept.

The Government has recognised that establishment of a national cyber-forensic facility could have the potential to improve law enforcement's capacity to deal with existing crime against or facilitated by computers and, more generally, would support the law enforcement community's knowledge and understanding of existing and emerging e-crime threats.

The Australian High Tech Crime Centre (AHTCC) has been established as a national centre for combating serious crime involving complex technology. The need for such a centre was a priority identified by the Australian Police Commissioners Conference in its Electronic Crime Strategy of March 2001 and endorsed by the Australasian Police Ministers' Council in November 2002.

The AHTCC is hosted by the Australian Federal Police (AFP) and staffed by AFP officers and State and Territory police officers seconded to the centre.

The role of the AHTCC is to provide a national coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes, especially those beyond the capability of single jurisdictions. The AHTCC is also tasked with assisting in improving the capacity of all jurisdictions to deal with high tech crime and support efforts to protect the National Information Infrastructure. The AHTCC will achieve this role through the provision of services that include coordination, investigation, intelligence, liaison, and knowledge.

The AHTCC will coordinate the consideration of high tech crime-related issues by Australian law enforcement agencies; investigate instances of high tech crime, independently or by way of cooperation with or referral to a partner agency; provide intelligence services that contribute to a better understanding of the high tech crime environment; act as a central point of contact in Australia for overseas law enforcement agencies; liaise with Government agencies, industry groups, businesses and other organisations on high tech crime matters; and act as a knowledge bank in relation to high tech crime issues, such as preventative measures, best practice investigative and forensic tools and techniques, training and education.

The AHTCC will therefore assist law enforcement agencies in setting best practice standards for computer forensic techniques through carrying out its core functions and through the operation of the Forensics Network, an association of police investigators with computer forensics expertise. The Forensics Network is being established under the auspices of the AHTCC and will include Commonwealth, State and Territory investigators.