Chapter 6

Further Developments and Conclusion

Recent initiatives

6.1 The world wide growth of information systems has resulted in new crimes and novel ways to perpetrate old crimes. As with any new development, the response to these crimes has been at first almost ad hoc. The Committee is reassured to find during the inquiry that a systemic approach is emerging.

6.2 The internet is a global phenomenon and any regulation of its use needs to be international to have the greatest impact. Internationally, the United Nations have addressed the issues and provided the parameters in which governments can usefully contribute to the regulation of an industry that offers great communication benefits to its citizenry.

6.3 Since the Committee commenced its Inquiry there have been some developments in the regulation of the Internet, both within Australia and internationally.

6.4 These include:

- introduction into Federal Parliament of the Spam Bill 2003; and
- the closure of certain internet chat rooms by Microsoft.

The Spam Bill 2003

6.5 The Spam Bill 2003 (the Bill) resulted from a report released by the National Office for the Information Economy in April 2003. In response, the government has developed a number of initiatives, including an information campaign, and legislation.

6.6 The legislation focuses on:

- the regulation of 'commercial electronic messages'; and
- the prohibition on the sending of unsolicited commercial electronic messages (commonly referred to as spam).

6.7 The Bill provides amendments to relevant legislation which will allow the Australian Communications Authority (ACA) as the overseeing body, to monitor commercial electronic message activity. It will also investigate complaints.

6.8 The scheme will also have enforcement provisions as well as provisions for the development of relevant industry codes and standards relating to commercial electronic messaging The ACA can institute proceedings in the Federal Court for breaches of the Act. Significant monetary penalties can be imposed, and the Court can order compensation where a party has suffered damage due to the breach.

6.9 From the evidence given and the submissions provided to the Inquiry one of the clear messages is that legislation or policy initiatives must have an international focus as well as a domestic application. The Explanatory Memorandum states:

> The proposed framework contained in the Bill is aimed at reducing Australia as a source of spam, minimise spam for Australian end-users and extend Australia's involvement in worldwide anti-spam initiatives.[1]

6.10 The Committee notes that the effect of the Bill is not intended to be confined to the domestic sphere but to contribute to international anti- spam initiatives.

Internet Chat Rooms

6.11 In Chapter Three of this report, there was discussion of the concern about the use of chat rooms, and the fact that control of their content and activities is impractical. On 24 September 2003, Microsoft announced it would close its chat rooms in 24 countries on 14 October. The company will not be closing services in the United States, Japan,New Zealand, Brazil and Canada which are subscriber-based. The subscriber-based services are paid for by credit card and therefore any illegal activity is traceable.

6.12 The Committee notes that Microsoft said that it wished to 'create a safer and more secure online experience and we want to protect families, in particular children, from unsolicited information and inappropriate communication online'.[2]

6.13 The Committee is also aware from the same press report that some experts believe that this would not necessarily make any difference to Internet safety, and disadvantages the 300,000 Australian users who will no longer be able to use this facility.

6.14 While not in any way detracting from the possible effect of Microsoft's action, it is possible that those who engage in criminal activities in chat rooms will simply use other technology such as mobile phones, which are increasingly capable of becoming communication centres with all of the capabilities of telephone, internet, video and television combined. The activity is likely to be diverted but not eliminated.

Conclusion and recommendations

The ACC and the AHTCC

6.15 The Committee considers that the roles of the Australian High Tech Crime Centre (AHTCC) and the Australian Crime Commission (ACC) in cybercrime detection and enforcement should complement each other. The ACC's role in

---

1 *Spam Bill 2003;* Explanatory Memorandum, p. 1

2 McLennan, David *'Shut chat rooms no help for net safety,'* The Canberra Times, 25 September 2003

collection and dispersal of intelligence is a part of its enforcement role function: the ACC is not a security agency.

6.16 The AHTCC's can support this role in its monitoring of the technological aspects of criminal activity, and keeping agencies apprised of the latest technology as well as the ways in which it might be used to commit crime. As two Commonwealth authorities, one of which includes the ACC the involvement of the State and Territory jurisdictions, there is the potential to establish a co-operative network of communication to act as a powerful weapon against cybercrime.

6.17 During the Inquiry the Committee's attention was drawn to an article by Michael Sussmann published in the Duke Journal of Comparative and International Law.[3] Sussmann summarises the challenges and the responses necessary to achieve cross-jurisdictional control of cybercrime. He notes that the former US Attorney General Ms Janet Reno outlined four critical areas for attention: legislation, commitment of personnel and resources, improved global abilities and an improved regime for collecting and sharing information.

6.18 The four categories apply equally to the three aspects of cybercrime under consideration, and provide a framework for the ways in which the ACC and the AHTCC might approach their roles.

Legislation

6.19 In an area such as cybercrime where new technologies are constantly being developed and taken up to facilitate crime, the regular monitoring of the adequacy of current legislation is essential to the success of enforcing the law against cybercrime.

Commitment of personnel and resources

6.20 As information technology becomes a part of the routine of everyday life, it will become part of crime. The current distinction between 'old' crime and e-crime will become blurred as it becomes a part of every crime. Without a commitment to training law enforcement personnel now, the capacity of LEA to respond to these developments will be diminished. Resources for education as well as those to ensure that the law enforcement bodies are apprised of all the available technological devices and information are necessary to meet this requirement.

Recommendation 7

The Committee recommends that the Government include in its cybercrime strategy, directed training for law enforcement agencies, and the development of a whole of government approach in which individuals can gain expertise which can be shared between those agencies.

---

3 Sussmann, Michael A. The Critical Challenges from International High Tech and Computer Related Crime at the Millennium [Vol 9:4511999]

6.21 Further, the Committee believes that education should include public education, as well as that of the law enforcement agencies.

Improved global abilities

6.22 Australia's acceptance of its role in the international arena was demonstrated during the inquiry. The recently introduced SPAM Bill (see paragraphs 6.5 to 6.9) acknowledges its responsibilities. Further, Australia's participation in the work of APEC is an example of the initiatives being undertaken in the global arena. In addition, the networks established by organisations such as the AFP, the AHTCC and the ACC are vital to Australia's participation in a consistent international approach.

Improved regime for collecting and sharing information.

6.23 The Committee has made recommendations in recognition of the need for a consistent national approach to ensuring that all relevant information is available to the agencies which need it. It is clear that there are opportunities for all law enforcement agencies to collect information on technology and crime and in doing so identify trends. Unless that information is shared, there is potential for duplication of activity leading to waste of resources and time. This is also contrary to the acknowledged need for a whole of government approach to combating cybercrime.

6.24 The Committee considers it is clear that isolated state or national action cannot succeed in controlling any other aspect of cybercrime unless there is a global commitment to a consistent regime of legislation and regulation. These areas for development can be applied at the local (multi- jurisdictional) Australian level, as well as the international level. With its international relationships with similar bodies, and its multi-state representation, the ACC is ideally placed to contribute to developing that regime, but not necessarily leading it.

Recommendation 8

The Committee recommends that the Australian Crime Commission continue its current level of involvement in cybercrime investigation, and intelligence gathering, as well as further developing its international liaison role.

Recommendation 9

The Committee recommends that the Australian Crime Commission ensure its information sharing strategies, including liaison with the Australian High Tech Crime Centre, maximise the opportunities for giving and receiving accurate and timely information about cybercrime methods and technology.

6.25 It became clear during the course of the hearings that there is no co-ordinating body which combines the role of watchdog, investigator, and prosecutor in this area. In his evidence to the Committee, Mr Melick said:

> The trouble is that there are too many players and no overarching coordinator.[4]

6.26 There is no organisation which is across all of the associated issues. While the Committee acknowledges that in other contexts combining these roles may not be desirable, the nature of cybercrime is such that rapid response is essential.

6.27 The Australian Federal Police submission noted that the new AHTCC has, as part of its role, to provide a national co-ordinated approach to combatting serious complex and/or multi-jurisdictional high tech crimes. In addition it also assists in improving the capacity of all jurisdictions to deal with high tech crime. The Committee is of the view that the AHTCC is in a position which would enable it to take a national perspective on cybercrime. However in order to develop this capacity, there must be a framework which supports it.

6.28 The Committee observed that Sussmann sets out this framework as including:[5]

- High technical standards which preserve public safety.
- The ability to preserve critical traffic data routinely, with powers to require a longer period of storage.
- The ability to share information across jurisdictions quickly – this requires legal processes supplemented by administrative procedures to facilitate the sharing of data.
- Government-Industry co-operation. This involves government minimising the compliance burden on industry, and simultaneously industry considering the public safety and interest as being a top priority.

6.29 From the Committee's observations of the evidence and the submissions provided, there are many ways in which LEA's, government agencies and the private sector are already working within Sussman's framework. However, it believes that further work can be done at all levels and in all spheres to develop strategies that will initiate innovative measures against cybercrime, and respond rapidly to instances of cybercrime. The complementary roles for the ACC and AHTCC can be identified in the following recommendations which are designed to promote partnerships in this process of Commonwealth and State governments as well as private industry.

Recommendation 10

The Committee recommends that the Australian Crime Commission seek out opportunities to participate in appropriate public/private sector cybercrime projects, to promote the sharing of information, and the efficient prevention and investigation of cybercrime offences.

---

4 *Committee Hansard*, 21 July 2003, p. 30

5 Sussmann, pp. 468 -469

Recommendation 11

The Committee recommends that the Australian High Tech Crime Centre act as a clearing house for information on cybercrime, in order to explore initiatives to combat it.

6.30 The Committee believes that the ACC can make an important contribution to the law enforcement agencies' understanding and prosecution of cybercrime in a number of ways:

- Through its statutorily authorised intelligence gathering function, the ACC can share its intelligence in the area with other agencies. In particular, through its Board, State Police can remain informed of these activities at the highest level.
- The ACC can work with the AHTCC on the prevention and investigation of cybercrime through the ACC's knowledge of the operational environment, and the AHTCC's knowledge of advancing technology.

6.31 The Committee observed with some optimism that developments in providing that protection are occurring in all areas: legislative, both private and public sectors, law enforcement agencies, and with the Internet Service Providers themselves. It is clear to the Committee that there are serious and sustained efforts being made to counter cybercrime, and the recommendations contained in this report are designed to enhance that effort.