Chapter 7

The adequacy of administrative and regulatory arrangements

Introduction

7.1 The inquiry revealed that certain administrative and regulatory arrangements hamper Australia's efforts to tackle serious and organised crime. One example is the inadequacy of the collection of prepaid mobile phone user information. The issue of staffing arrangements for law enforcement agencies was also investigated, as was the need for a comprehensive research effort to improve future policing strategies and the targeting of policy and resources to address serious and organised crime in Australia.

Telecommunications

SIM card user registration[1]

7.2 During the inquiry, the committee's attention was drawn to failings in the current arrangements for registering user information for prepaid mobile phone SIM cards. These are governed by a telecommunications industry determination made under a model of self regulation.

7.3 The committee received significant evidence from several law enforcement agencies about the potential and actual use of SIM cards by organised crime groups to avoid detection, whereby criminal identities are purchasing SIM cards in stolen or false names. The Queensland Crime and Misconduct Commission submission notes:

> Prepaid SIM cards are regularly purchased and used by target identities (including in bulk) in false names or in the names of real persons without the knowledge of the person in question. A number of proprietors of mobile telephone outlets, and some smaller service providers, have been implicated in activity of this type. Initiatives by the Commonwealth Government-sponsored Law Enforcement Advisory Committee (LEAC) have experienced difficulties keeping pace with criminal activity in this area. This has tangible and ongoing effects on the ability of agencies to target organised crime and other related activity.[2]

7.4 Detective Superintendent Kim Porter, Divisional Superintendent, Organised Crime Division, Western Australia Police, told the committee that where criminals are aware that the police are tracking them they will change their cards 'two, three, four

[1] SIM is an acronym for Subscriber Identity Module. A SIM is a small card to hold subscriber details and an electronic password: Australian Communications and Media Authority, http://toolkit.acma.gov.au/mobile/glossary.htm, viewed 5/09/2007.

[2] *Submission 8*, p. 11.

times a day', and possibly 'every second conversation'. There will either be no name attached to the purchase, or the purchaser will have supplied a false one.[3]

7.5 Ms Elizabeth Foulger, Manager, Intelligence, Queensland Crime and Misconduct Commission, reported a similar experience, exacerbated for her agency by the fact that, in the absence of state telephone interception powers, the commission relies heavily on charge record analysis:

> …you can clearly see phones that have been connected using false names…We see ridiculous names like Will Smith and Bob Marley—clearly names that have been plucked out of the air. There is no process in place at the moment to prevent that from happening.[4]

7.6 The Western Australia Police (WAPOL) estimated that 50 per cent of telephone numbers they investigate have false subscriber details, with the majority of these false accounts being drug related.[5]

7.7 Detective Superintendent Mark Porter, State Intelligence Division, Victoria Police, put the use of SIM cards in a commercial criminal context, telling the committee that the 'churning' of SIM cards emerged around a decade ago. While briefly restricted to 'top end' criminals, this is now a widespread practice among the criminal fraternity. Detective Superintendent Porter observed that the need to communicate is fundamental to any business—legitimate or not. Accordingly, criminals tend to treat the cost of obtaining secure communications as a 'business' cost:

> So, if…[a criminal goes] in and buy[s] 100 SIM cards, that is a business cost, because…[their] riskiest point is…[the] point of communication'.[6]

7.8 Further, Ms Foulger told the committee that some organised crime figures have links to the providers of mobile phones, and are able to obtain phones using the legitimate details provided by unsuspecting third parties. For law enforcement, tracking down the actual user of a service becomes very difficult.[7] In some cases, organised crime groups are endeavouring to establish control over the commercial supply of SIM cards by establishing, purchasing or otherwise controlling their own telecommunications companies. Detective Superintendent Porter told the committee:

> Another reason why you need to legislate is…they buy their own telephone suppliers so that they can get those cards without having to answer the questions. The situation is that we need to have legislation to make sure that the actual supplier is required to comply.[8]

[3] *Committee Hansard*, 30 April 2007, p. 17.

[4] *Committee Hansard*, 7 June 2007, pp 47-48.

[5] Western Australia Police, *Submission 15*, p. 5.

[6] *Committee Hansard*, 1 May 2007, p.19.

[7] *Committee Hansard*, 7 June 2007, pp 47-48.

[8] *Committee Hansard*, 30 April 2007, p. 22.

100-point identity checks

7.9 The accurate collecting of SIM user information is critical to law enforcement agencies' ability to investigate serious and organised crime. Detective Superintendent Porter observed that current arrangements are allowing criminals to obtain effectively anonymous means of communication:

> When you can go into the supermarket and buy quite a number of…[prepaid mobile services] and you can just make a phone call and claim to be anybody, then you have anonymous identification that you can use for five minutes, five days or whatever.[9]

7.10 The Western Australia Police submission notes:

> The fact that telecommunication service providers do not require or impose the 100 point identification check on the purchase of SIM cards makes identifying the actual user virtually impossible.[10]

7.11 The Australian Mobile Telecommunications Association (AMTA) responded to the evidence received regarding SIM cards and prepaid mobile service registration. Their submission outlines that the *Telecommunications (Service Provider—Identity Checks for Pre-Paid Mobile Telecommunications Services) Determination 2000* applies to the sale of prepaid mobile phones, and that there are established processes for collecting and verifying customer information.

7.12 Under the determination, purchasers of SIM cards are required to produce identity documents either when purchasing a prepaid mobile phone (option A) or when activating a prepaid mobile service (option B). The submission, acknowledging the shortcomings of the present approach, continues:

> Industry’s preference would be to use option B above, but transition to this process has been consistently thwarted by the lack of access to original sources for verification of customer provided information. As a result, option A is used, with suboptimal outcomes, including:
>
> 1. incomplete or no collection and verification of customer data at some retail outlets
>
> 2. differences between the information collected from the purchaser and the user (e.g. if the mobile is a gift)
>
> 3. incomplete and unverified data in the IPND,[11] as this data is collected from the user at service activation.[12]

[9] *Committee Hansard*, 1 May 2007, p.19.

[10] *Submission 15*, p. 5.

7.13 The AMTA submission also explains proposed improvements to the collection of SIM purchaser information:

> AMTA members are developing a standard form for pre-paid mobile phone services in order to seek more accurate and consistent data capture at point of sale. To complement the development of the new pre-paid mobile phone service form, AMTA is developing an overall continuous improvement process that consists of comprehensive guidelines for retailers and an education program upon roll out of the new form.[13]

7.14 AMTA suggests that the identity checks could be undertaken at the point of activation (option B above), and suggests that the government's proposed National Document Verification Service (NDVS) could be used to support such an approach.[14] The NDVS is a part of the National Identity Security Strategy developed by the Council of Australian Governments; a national prototype was tested in 2006. The NDVS:

> …will be a secure, electronic, on-line system accessible by all key Australian Government, State and Territory agencies, and potentially by the private sector. Agencies authorised to use the DVS will be able to check in real time whether a document presented to them as a proof-of-identity by an individual applying for high value benefits and services was issued by the relevant agency, and that the details on the document are true and accurate.[15]

Implications of a deregulated market

7.15 While the committee notes AMTA's willingness to assist with the support of the NDVS, there is no indication of when the database will become operational. In AMTA's view, the 100-point check is an 'outdated' form of identification, specifically because the deregulated telecommunications market has resulted in there being less control over call records. This makes it difficult to ensure that complete and accurate records are created.

[11] The Integrated Public Number Database (IPND) is an industry-wide database that contains information on all listed and unlisted public telephone numbers in Australia, regardless of the service provider. The IPND came into operation on 1 July 1998 and is maintained by Telstra under the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*: Department of Communications, Information Technology and the Arts, http://www.dcita.gov.au/communications_and_technology/policy_and_legislation/numbering/integrated_public_number_database_(ipnd), viewed 31 July 2007.

[12] Australian Mobile Telecommunications Association, *Submission 22*, p. 2.

[13] *Submission 22*, p. 2.

[14] *Submission 22*, p. 3.

[15] Attorney-General's Department, http://www.ag.gov.au/www/agd/agd.nsf/page/Crimeprevention_Identitysecurity#q2, viewed 31 July 2007.

7.16 This was also noted by Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department, who told the committee:

> Because it is a deregulated telecommunications market, the obligation has been placed upon industry to come up with how that area is regulated.[16]

7.17 Ms Smith referred to the telecommunications determination of 2000, identified above, and continued:

> The difficulty is that there is no regulation of who can sell those SIM cards. Even though an obligation may be placed on the main telecommunications providers who provide them, they are sold at the local garage, at Woolworths and so on, so the obligation might fall upon a checkout person, who is very busy, to take down certain details and that sort of thing…In the Law Enforcement Advisory Committee, which is chaired by ACMA, we have been working very hard for a number of years to come up with a better system. We expect that—I think in July this year—AMTA will be putting out a new draft way to deal with these prepaid SIMS. So something is being done.[17]

Implications for commercial and consumer interests

7.18 The committee considers that prompt and serious attention must be given to ensuring that reliable records of mobile phone users are created and kept. Apart from data and information acquired through telecommunications interception under warrant, law enforcement agencies rely heavily on this data from telecommunications companies. While the committee recognises the potential for greater regulation to be a considerable impost on telecommunications providers and consumers, the lack of access to reliable SIM user information is seriously undermining the ability of police to detect, investigate and prosecute organised crime groups. The advantages of a deregulated telecommunications market must therefore be tempered by a system of obtaining accurate SIM user information. The committee's support for stricter proof-of-identity requirements is given with recognition that, ultimately, the success of any system will be judged by how well commercial and consumer interests are preserved within a system that achieves comprehensive and accurate SIM card user registration.

7.19 The committee acknowledges that any changes to the current model for obtaining registration of SIM card users have the potential to affect the administrative and commercial performance of telecommunications providers. Stricter requirements around purchasing SIM cards could add to the length and cost of transactions and potentially affect sales.

7.20 Equally, additional inconvenience and expense could adversely affect individual consumers, and the committee notes the significant practical considerations

[16] *Committee Hansard*, 5 July 2007, pp 17-18.

[17] *Committee Hansard*, 5 July 2007, pp 17-18.

that would arise with a requirement to provide 100 points of identity documentation for purchase or activation of SIM cards. Young people in particular might find tougher requirements difficult to satisfy, if not an outright barrier to ownership, and the effect on consumers of any proposed changes should be directly addressed in establishing a more effective system.

Recommendation 9

7.21 The committee recommends that the government seek to expedite the telecommunications industry's adoption of option B of the *Telecommunications (Service Provider—Identity Checks for Pre-Paid Mobile Telecommunications Services) Determination 2000,* so as to require 100 points of identity documentation upon activation of prepaid mobile phone services.

Voice over Internet Protocol

7.22 The committee heard that rapid technological change in the telecommunications industry is a continuing threat to the ability of law enforcement agencies (LEAs) to capture telecommunications information. In particular, Voice over Internet Protocol (VoIP) does not require billing records. Mr Christopher Keen, Director, Intelligence, Queensland Crime and Misconduct Commission, described the nature of the problem and how it impacts upon the usual lines of inquiry:

> …through things like voice-over-internet protocol, we do not know where...[a call] went. You just pay your $50 up front and, therefore, they no longer need billing records…[I]t is having an impact on us being able to salvage networks, links and then, from there, perhaps taking some other action.[18]

7.23 Ms Smith advised the committee that, because the relevant Acts in this area—the *Telecommunications (Interception and Access) Act 1979* and the *Telecommunications Act 1997*—are 'technology neutral', carriers have the same reporting obligations around VoIP as they do for fixed line services.[19] Nevertheless, Ms Smith acknowledged that there are 'challenges' to be addressed arising from the need to deal with and rely on the many players making up the telecommunications industry, such as smaller and overseas providers. These, as well as technological issues, are being examined.[20]

7.24 The committee is concerned that technological developments will make it more difficult for LEAs to identify and pursue criminal identities, and will monitor the department's initiatives for dealing with this area of concern.

[18] *Committee Hansard*, 7 June 2007, p. 51.

[19] *Committee Hansard*, 5 July 2007, p. 20.

[20] *Committee Hansard*, 5 July 2007, p. 20.

Staffing of intelligence and law enforcement agencies

Targeting of human resources to organised crime

7.25 The committee heard evidence that police efforts to combat organised crime are still vulnerable to compromise by traditional policing responsibilities. Investigation of organised crime is typically complex, labour intensive and long term, and it can be interrupted by the requirements of day-to-day policing—particularly when resources are urgently directed to ad hoc high-profile cases or investigations.

7.26 To an extent, Australia has taken the first important steps to separate these two areas of policing with the creation of specialist crime and corruption bodies such as the ACC. As the Corruption and Crime Commission of Western Australia (CCCWA) has observed:

> Within Australia a number of Royal Commissions have been established to investigate and report on organised crime. Emerging from these commissions has been the recognition that traditional policing methods were inadequate and new arrangements for combating organised crime were needed.[21]

7.27 The CCCWA endorsed Australia's current model for dealing with organised crime, which enables resources and effort to be dedicated to long-term strategies:

> Establishing alternative working arrangements offers government an opportunity to 'quarantine' resources for the long-term protracted investigations that are the trademark of effective organised crime investigations, rather than having these resources dispersed, responding to day-to-day policing issues.[22]

Staff retention, expertise and inter-jurisdictional mobility

7.28 The inquiry identified a present tendency for law enforcement agencies to experience high staff turnover and lose valuable professional experience and corporate knowledge. This problem is particularly acute given the increase in technology enabled or facilitated crime, and the rapidity with which criminals are exploiting new technology. Professor Rod Broadhurst, appearing before the committee in a private capacity, explained:

> We do have a terrible shortage of expertise. The kind of expertise that you are talking about is hard to keep. We have had entire forensic computing sections of police forces get up and resign and go and work in private

[21] Corruption and Crime Commission of Western Australia, 'Organised crime report to the Joint Standing Committee on the Corruption and Crime Commission with regard to the Commission's organised crime function and contempt powers', December 2005, p. 8.

[22] Corruption and Crime Commission of Western Australia, 'Organised crime report to the Joint Standing Committee on the Corruption and Crime Commission with regard to the Commission's organised crime function and contempt powers', December 2005, p. 8.

> enterprise. We have people who are trained poached by the big IT security firms.[23]

7.29 Commissioner Ken Moroney, NSW Police Force, described one of the factors behind staffing movements as competition for skills from certain industries or sectors:

> Certainly in some of our highly specialised information technology areas we are losing police officers, ironically, to the Commonwealth, which perhaps is in a position to offer better salaries, better salary packages and a diversity of work away from strict law enforcement. One of our senior IT police officers has recently been employed by the Department of Defence. A range of issues were taken into account in that career path—different opportunities and salary were certainly key issues. Those are salaries that, in one sense, I cannot compete with. We are losing them also to the private sector.[24]

7.30 Mr Mark Burgess, Chief Executive Officer, Police Federation of Australia (PFA), indicated that police skills are a useful, marketable and valuable commodity in the current employment market.[25]

7.31 Mr Burgess advised that, while inter-jurisdictional mobility is desirable within an integrated and coordinated national approach to policing organised crime, there is a need for a more systematic approach to staff secondment and transfers. This would ensure that state agencies are not continually affected by shortages of labour and/or skill.

7.32 The PFA warned that Australia requires the recruitment of some 13,000 new officers to meet the existing commitments of state and territory police forces.[26] While the PFA did not endorse a central recruiting pool as the way to manage staffing nationally, it did support the funding of a 'national police workforce planning study' to ultimately form the basis of a national police workforce strategy.[27] The PFA believes that such a coordinated approach could secure effective national management and planning of police staffing levels, while maintaining the positive aspects of inter-jurisdictional mobility within the service, and respecting the self-determination of individual police agencies.

7.33 Commissioner Mick Keelty, Australian Federal Police (AFP), pointed to both individual factors and general international trends as causing staffing pressures on Australian police forces:[28]

[23] *Committee Hansard*, 7 June 2007, p. 68.

[24] *Committee Hansard*, 8 June 2007, p. 13.

[25] *Committee Hansard*, 5 July 2007, p. 48.

[26] *Committee Hansard*, 5 July 2007, p. 46.

[27] *Committee Hansard*, 5 July 2007, pp 41-46.

[28] *Committee Hansard*, 5 July 2007, p. 60.

> In terms of…overall policing numbers…retaining staff is an issue at the national level. There are various reasons why police organisations do not retain staff. I have spoken to Commissioner Paul White in the Northern Territory and we have talked about the difficulties of policing in the Northern Territory—the remoteness of it and the lack of familial connections. I have talked to my counterpart in Queensland, Bob Atkinson. Bob unashamedly will tell you that a lot of police want to come and work in Queensland. Some of it is the social demographics of Australia. In Western Australia, despite the perception that the AFP has stolen their staff, a lot of the police staff have actually gone to the mining industry.[29]

7.34 Commissioner Keelty observed that, although staff movements occur in all directions between state and territory forces and the private sector, the AFP does not experience the staff retention problems of the state and territory police forces.[30] This is due to the diversity of work that the AFP undertakes, which offers greater professional choices to staff.[31] While the AFP does not actively recruit members of state and territory police forces, there is a natural gravitation toward its ranks.

7.35 Mr Tony Harrison, Assistant Commissioner, Crime Service, South Australia Police, while acknowledging the value of inter-agency mobility for skills development and cross-pollination of ideas, observed that the preponderance of such movements is from state or territory to Commonwealth agencies, notably the AFP and the ACC.[32]

7.36 The committee believes that, without adequate recognition, planning and effort, police can expect to continue to encounter shortages of skills and personnel.

Recommendation 10

7.37 The committee recommends that the Ministerial Council for Police and Emergency Management—Police consider a more strategic and national approach to recruitment and retention of sworn police officers across all jurisdictions; and that consideration be given to enhancing cross-jurisdictional mobility, including secondments, of sworn police officers and other police service personnel.

Numbers of sworn Australian Federal Police

7.38 The PFA also raised concerns about the numbers of sworn police officers in the AFP, as only sworn officers can undertake the full range of policing activities. Mr Burgess considered that this could affect an agency's capacity to fulfil its responsibilities and that, despite recent increases in the AFP's staffing budget and overall numbers, the proportion of sworn AFP officers has declined. In light of the increases in AFP responsibilities, such as anti-terrorism activities and investigations,

[29] *Committee Hansard*, 5 July 2007, p. 59.

[30] *Committee Hansard*, 5 July 2007, p. 62.

[31] *Committee Hansard*, 5 July 2007, p. 60.

[32] *Committee Hansard*, 6 July 2007, pp 24-25.

there is an expectation that fully sworn officers will attend to matters of serious and organised crime.

7.39 In reply to the PFA's suggestions, Commissioner Keelty advised the committee that the increase in unsworn staff recruited to the AFP is properly viewed as a reflection of the type of skills required by the organisation. In particular, the AFP has increased the size of its intelligence area, in which it is suitable for unsworn staff to be employed.[33]

7.40 Commissioner Keelty raised the related issue of police pursuing partnerships with community and private sector groups. This approach is in use or being considered by countries overseas, such as the US and UK. The use of 'enthusiastic' and properly skilled people to free-up sworn officers to undertake critical tasks could help with the management of staffing and skills pressures.[34]

Developing evaluation and research to inform policy and policing strategies

Evaluation

7.41 Attempts to address the impact of serious and organised crime effectively are held back by reliance on an unstructured and almost reactive approach to considering policy design and funding choices for law and order regimes. Improved systems of measuring outcomes will allow Australia to bridge the chasm between the political concerns that so often shape policy development and the practical imperatives of a system of laws that is effective against organised crime.

7.42 Professor Adam Sutton, appearing in a private capacity, identified the Productivity Commission as the agency best placed to undertake such an inquiry:

> …I would argue very strongly for the Productivity Commission. Most areas of government now, quite rightly, are tied to those kinds of [Productivity Commission] performance objectives. I do not think we are doing that in the law enforcement area…partly because of this idea of intelligence data being privileged, secretive et cetera.[35]

7.43 The Productivity Commission is an independent Commonwealth agency that acts as:

> …the Government's principal review and advisory body on microeconomic policy and regulation. It conducts public inquiries and research into a broad range of economic and social issues affecting the welfare of Australians.

[33] *Committee Hansard*, 5 July 2007, p. 59.

[34] *Committee Hansard*, 5 July 2007, p. 65.

[35] *Committee Hansard*, 1 May 2007, p. 11.

> The Commission's work covers all sectors of the economy. It extends to the public and private sectors and focuses on areas of Commonwealth as well as State and Territory responsibility.[36]

7.44 The committee considers that there is a need for evaluative research to quantify the effectiveness of current policy and legislative and administrative arrangements for serious and organised crime, as currently exists in other areas of large public investment.

7.45 The committee has also commented in previous inquiries on the difficulties of establishing performance objectives for law enforcement that adequately reflect its work and outcomes. Accordingly, the committee would support a Productivity Commission inquiry into the effectiveness of current arrangements to address serious and organised crime.

Recommendation 11

7.46 The committee recommends that the Productivity Commission inquire into the cost effectiveness and benchmarking of law enforcement bodies and current national arrangements to address serious and organised crime.

The importance of research in fighting organised crime

7.47 In bringing together policymakers and legislators, LEAs, academics and research bodies, the inquiry demonstrated the value of multidisciplinary or collective approaches to examining and assessing the character and activities of organised crime. Mr Alastair Milroy, Chief Executive Officer, Australian Crime Commission, observed:

> The ACC values the important dialogue that has arisen through this inquiry. It is through this varied and informed debate involving law enforcement agencies, academia, politicians, the legal community and concerned citizens that Australia can better arm itself to combat the continuing scourge of serious and organised crime.[37]

7.48 Mr Milroy called for a greater involvement and contribution by academia to the body of research informing Australia's policy and operational choices in fighting organised crime:

> …academia has done some work that looks at the characteristics of organised crime. But even our partners in the UK have acknowledged that a lot of that work needs to be done by others to give us better advice on what can be done from a government point of view in tackling organised crime.[38]

[36] Productivity Commission, http://www.pc.gov.au/commission/charter.html, viewed 21 August 2007.

[37] *Committee Hansard*, 6 July 2007, p. 27.

[38] *Committee Hansard*, 6 July 2007, p. 34.

7.49 Mr Milroy pointed to certain areas of potential research where better understanding is needed:

> …a lot more work could be done to fill in some of the gaps…[such as] the value of organised crime markets, which is about the revenue derived by organised crime in pursuit of illegal activity…To deal with organised crime, to assist in forming policy and to have better operational responses, you have to look at the problem itself and understand organised crime markets.[39]

7.50 Experiences under the current national policing arrangements for organised crime have shown that the best strategic and tactical options can only be selected when police can accurately identify the groups and actors causing the greatest levels of threat and harm in the community, and the markets and activities in which they are involved. Given the acknowledged flexibility and opportunism of organised crime groups, research is also required to support analysis of successful policing strategies. This would allow police to better anticipate new markets or criminal strategies:

> …with organised crime, once you are successful in targeting specific groups, they learn from it and change their methodology. It is an ongoing cycle of us trying to learn from their various operations, looking at the intelligence, identifying the methodology that they are using and looking at how their businesses are structured.[40]

7.51 Mr Frank Costigan QC, who appeared before the committee in a private capacity, emphasised that a research effort would need to be ongoing in order to inform and develop appropriate police responses to the opportunism and continuing evolution of organised crime:

> There is no clear-cut answer to these things; it is a continuing fight. As new methods of attack are found, there will be new methods of getting around the system.[41]

7.52 Professor Margaret Mitchell, Director, Sellenger Centre for Research in Law, Justice and Policing, School of Law and Justice, Edith Cowan University, supported the analyses of Mr Milroy and Mr Costigan. So too, Dr Toni Makkai, Director, Australian Institute of Criminology, observed that 'one of the difficulties or challenges for…[the Australian Institute of Criminology] is getting our research to influence policy and practice'.[42] This has serious implications for the development of policy and effective practical and legislative strategies in Australia:

> …if we do not have these linkages, if we are not able to get policymakers and practitioners to take notice of the research and the evidence base, we

[39] *Committee Hansard*, 6 July 2007, p. 33.

[40] Mr Alastair Milroy, Chief Executive Officer, Australian Crime Commission, *Committee Hansard*, 6 July 2007, p. 34.

[41] *Committee Hansard*, 1 May 2007, p. 38.

[42] *Committee Hansard*, 5 July 2007, p. 86.

> will not be able to improve the efficiency and effectiveness in terms of our responses to serious and organised crime in Australia.[43]

7.53 Professor Mitchell identified this failure to incorporate research into policy and policing strategies as international in nature, and called for a 'careful and comprehensive overview, analysis and synthesis of the nature of the problem', observing:

> Despite real concern over the increasing threat from organised crime, there is very little rigorous analysis of its nature, scale and impact.[44]

7.54 Professor Sutton noted the need for improved evaluation of organised crime, and for research to be informed by police operational information. This would allow research to inform and thereby improve the strategies and direction of police agencies:

> I do not see that there is any reason that, if you could link police intelligence with research, you could not actually measure that and use that in a feedback loop in order to guide your operation.[45]

7.55 The committee endorses the argument that, without sound research on the precise nature and effects of organised crime, policymakers and practitioners will be hampered in producing efficient and effective responses to organised crime.

Current research collaboration in Australia

The Australian Institute of Criminology

7.56 The committee received evidence showing some important, if nascent, collaborative efforts between police and information and/or research agencies, such as the Australian Institute of Criminology (AIC) and CrimTrac.

7.57 Dr Makkai explained that the AIC has a 'close working relationship' with bodies such as the ACC and the Attorney-General's Department, whereby the AIC both informs and comments on intelligence matters from a research perspective. Notably, the AIC provides input, by way of confidential comment, to the ACC's *Picture of criminality in Australia* report.[46]

7.58 Putting this in context, Dr Makkai explained that much of the AIC's work is commissioned or contracted, with it having to carefully allocate its $5.3 million budget to other projects.[47] The recent and current projects of the AIC show its work to be highly relevant to the matters central to the committee's inquiry. These include high-tech crime, implementation of the *Anti-Money Laundering and Counter-*

[43] Dr Toni Makkai, Director, Australian Institute of Criminology, *Committee Hansard*, 5 July 2007, p. 86.

[44] *Committee Hansard*, 30 April 2007, p. 34.

[45] *Committee Hansard*, 1 May 2007, p. 6.

[46] *Committee Hansard*, 5 July 2007, p. 84.

[47] The AIC contracted over $2.5 million of work in 2006.

Terrorism Financing Act 2006, online child pornography, drug analysis of detainees and emerging illicit drug trends.[48]

7.59 Currently, links between research and police agencies are largely informal. However, the AIC is assiduous in the number and variety of methods it employs to promote closer links:

> We have been trying to…[collaborate] through the informal exchange of information and knowledge…We have been locating our analysts in policy and in the operational environments so that they get better informed and they can then inform the people they are working with about the latest research and what it is showing.
>
> We have run a series of closed roundtables so that law enforcement in particular can come together and talk about things in a confidential way, not in the public arena. We also run open public conferences on issues. We do the standard thing of publishing our material. We also have moved towards trying to do shorter facts sheets…which are much shorter, we hope, easier to read and more targeted on a specific issue and, therefore, they will be more likely to be picked up, particularly by practitioners but also by busy policymakers.[49]

7.60 In addition, the AIC has considerable professional affiliations with national and international bodies:

> [The AIC sits] on a number of national boards and councils, such as the Australian National Council on Drugs and National Crime Stoppers. We participate internationally through the program network institutes of the UN and we attend the UN Crime Commission meetings as part of the delegation led by the Attorney-General's Department.[50]

7.61 Despite these efforts to establish more extensive and valuable collaboration, Dr Makkai stated that there is still the need for improved links between LEAs and the research sector:

> …[The AIC does] not have routine access to either Commonwealth or state and territory criminal justice databases. To a certain extent, our capacity to produce new and innovative research is dependent on these agencies enabling access to the relevant materials.[51]

7.62 Mr Bob Bottom, appearing in a private capacity, identified the lack of a formally structured research program designed specifically to marry relevant research with policy and policing outcomes as a significant weakness in addressing organised

[48] Dr Toni Makkai, Director, Australian Institute of Criminology, *Committee Hansard*, 5 July 2007, pp 85-86.

[49] Dr Toni Makkai, Director, Australian Institute of Criminology, *Committee Hansard*, 5 July 2007, p. 82.

[50] Dr Toni Makkai, Director, Australian Institute of Criminology, *Committee Hansard*, 5 July 2007, p. 86.

[51] *Committee Hansard*, 5 July 2007, p. 85.

crime in Australia. Mr Bottom pointed to the UK, where the Serious and Organised Crime Agency (SOCA) has developed an annual public document outlining the nature of organised crime in that country.[52] SOCA has also established a research program designed to provide objective support for the development and pursuit of SOCA's policing and policy strategies.[53]

7.63 Mr Bottom argued that Australia needs a similar program 'to provide research evidence to support the development of policy and practice relating to the [reduction] of organised crime'.[54] This need is heightened by the existence of the ACC, which, operating with a truly national structure and focus, requires a substantial foundation of information, knowledge and analysis from which to plan and coordinate its activities, and by which to assess and measure the success of its performance.

7.64 Throughout the hearings, the committee explored the notion of underpinning law enforcement efforts with complementary research projects. In general, witnesses supported such an approach. For example, Mr Keen advised:

> [A targeted research effort]…certainly is conceptually a very good idea. Whichever agency or person comes up with it, there is going to be the need for a fair amount of academic rigour, so you are probably almost looking at a special project to do that.[55]

7.65 The committee supports the provision of comprehensive research to support law enforcement in the area of organised crime, and believes that the AIC is well placed as a Commonwealth statutory authority to undertake this role.

Recommendation 12

7.66 The committee recommends that the Commonwealth Government increase funding to the Australian Institute of Criminology.

Recommendation 13

7.67 The committee recommends that a formal relationship be established between law enforcement agencies, government departments and the Australian Institute of Criminology to enhance the provision of data, information and research; and that particular emphasis be placed on the removal of any legislative impediments to the provision of data to the Australian Institute of Criminology by Commonwealth, state and territory departments and agencies.

Research and education

7.68 The committee believes that the establishment and use of a research effort to complement and inform the priorities, strategies and outcomes of law enforcement

[52] *Committee Hansard*, 7 June 2007, p. 29.

[53] *Committee Hansard*, 7 June 2007, p. 29.

[54] *Committee Hansard*, 7 June 2007, p. 29.

[55] *Committee Hansard*, 7 June 2007, p. 54.

efforts can provide a base from which to coordinate education activities around crime and organised crime, such as in the area of illicit drugs.

7.69 The committee heard evidence that there is still a gulf between social attitudes toward some drugs, nominally 'recreational', and the serious harms that can flow from even casual instances of illicit drug use.[56] As part of a future crime prevention strategy, Mr Keen identified the need for a coordinated research effort to provide targeted and well-designed educational programs:

> …what we need…[is] a short, sharp, shiny description of what to look for and what the impacts are—and try to get some of those out [in education campaigns]…[T]here is an enormous part of the market that we are not even touching as far as education goes.[57]

7.70 Some witnesses saw education as an important tool in the area of high-tech crime. Where technology is employed or taken advantage of in furtherance of criminal activities, better education of technology users is needed to complement enforcement initiatives. In this respect, Mr Rob McCusker, a research analyst in transnational crime for the Australian Institute of Criminology, observed:

> The difficulty…in all approaches to tackling technology involving crime is that we still have a massive gullible public who make the job extremely difficult. Until we can tackle that issue through education campaigns and so forth, law enforcement efforts in this area will be constantly scuppered.[58]

7.71 The committee notes that the Commonwealth Government has invested substantially in drug education.[59] However, in light of the detrimental effects of serious and organised crime in other sectors of society, it is the committee's view that investment in public education in areas related to high-tech crime is necessary.

Recommendation 14

7.72 The committee recommends that public education programs about emerging criminal activities, such as credit card fraud, banking fraud, identity theft and internet-based criminal activity, be given a higher priority and increased resources.

Picture of criminality in Australia report

7.73 Calls for 'a more coordinated approach to research on organised crime in Australia' were consistently made throughout the inquiry.[60] In particular, some

[56] *Committee Hansard*, 7 June 2007, p. 54.

[57] *Committee Hansard*, 7 June 2007, p. 54.

[58] *Committee Hansard*, 5 July 2007, p. 89.

[59] See Parliamentary Joint Committee on the Australian Crime Commission, *Inquiry into the manufacture, importation and use of amphetamines and other synthetic drugs (AOSD) in Australia*, February 2007.

[60] Mr Bob Bottom, Private Capacity, *Committee Hansard*, 7 June 2007, p. 28.

witnesses called for this to be established around the annual preparation and public release of a declassified version of the ACC's *Picture of criminality in Australia* (PoCA) report. The PoCA is 'a confidential high-level strategic intelligence report on the relative harms of each crime type, emerging issues in the criminal environment and strategic threats from various issues in the surrounding region', and is the ACC's central strategic document.[61] Mr Bottom expressed bemusement and some disappointment there had been no implementation of a recommendation on this issue in this committee's report on the ACC's 2004-05 annual report.[62] That recommendation was:

> …that the Australian Crime Commission consider the release of public versions of key research, including a declassified version of the Picture of Criminality [in Australia report].[63]

7.74 Mr Bottom told the committee that release of a declassified version of PoCA is desirable because it would act as a focus and anchor for public information and debate about crime going into the future. Mr Bottom observed that the PoCA's substance goes to the very heart of the committee's current inquiry, and it could be an invaluable resource.[64]

7.75 Mr Bottom explained that a declassified version of PoCA could ensure that an appropriately Australian perspective was maintained when considering and designing responses to crime and the anticipated requirements of LEAs. There was, he said, an over-reliance on overseas data and European perspectives, both in Australia generally and, in particular, in much of the evidence that had been received by the inquiry:

> …I refer to the submission from the Australian Institute of Criminology…[N]ot one of its 16 references credited…is from Australia; indeed, not even from the AIC itself, which in recent years, to its credit, has produced two of the best academic or research based assessments of organised crime within Australia. The tendency, therefore, of academics to ignore such local research and point you to Europe is, to put it mildly, an unfortunate example of academic naivety.[65]

7.76 Apart from the obvious benefits of basing Australian strategies on Australian experiences and data, Mr Bottom pointed to the fact that Australia has been a leader in the establishment of ACC type bodies, and has, for example, provided the model for the establishment of the Serious and Organised Crime Agency in the UK. To look to

[61] Parliamentary Joint Committee on the Australian Crime Commission, *Examination of the Australian Crime Commission Annual Report 2005-06*, June 2007, p. 16.

[62] *Committee Hansard*, 7 June 2007, p. 26.

[63] Parliamentary Joint Committee on the Australian Crime Commission, *Examination of the Annual Report 2004-2005 of the Australian Crime Commission*, p. vii.

[64] *Committee Hansard*, 7 June 2007, pp 30-31.

[65] *Committee Hansard*, 7 June 2007, p. 28.

overseas models therefore appeared to him retrograde and unlikely to provide many meaningful comparisons or insights.[66]

7.77 The committee notes that the previous recommendation for a declassified or public version of the PoCA is still awaiting a response by the government; this was also noted in the committee's June 2007 report on the ACC annual report for 2005-06. As stated there, the committee looks forward to receiving the government's response to this recommendation.

7.78 Mr Milroy took the opportunity of appearing before the committee to address the issue of the delayed release of a declassified version of the PoCA:

> The ACC…wishes to respond to criticism concerning the release of the public version of the ACC's picture of criminality in Australia. We are in the final stages of developing a paper, which is termed *Organised crime in Australia*, following extensive consultation with our partners and this will be delivered to the ACC board this month for their consideration for release to the public.[67]

7.79 The committee commends the ACC on this development.

The Committee notes that the ACC has prepared a public version of it picture of criminality in Australia and recommends

Recommendation 15

7.80 The committee notes that the Australian Crime Commission has prepared a public version of the *Picture of criminality in Australia* and recommends that the ACC Board make this report available at the earliest possible date.

Reporting online fraud

7.81 A related issue to emerge from the committee's consideration of the question of establishing a complementary research effort for Australian police agencies was that of the reporting of online fraud in Australia. A number of witnesses saw the current approach to reporting online fraud as being inadequate.

7.82 Dr Makkai advised the committee that, in respect of technology-based or high-tech crimes, a lack of reliable data and 'data infrastructure' means that research in this area is not well developed, especially in comparison to traditional types of crime, such as property and violent crime:

> Certainly from a research perspective we would like to know the data…[High-tech crime] is, for example, one of those crimes that we know is grossly underreported to police and, as a consequence, we do not have

[66] *Committee Hansard*, 7 June 2007, p. 29.

[67] *Committee Hansard*, 6 July 2007, p. 29.

> any idea of the size of the problem. As researchers, we would welcome much better data.[68]

7.83 Mr Alexander Webling, Senior Adviser, E-Security Strategy, Critical Infrastructure Protection Branch, Attorney-General’s Department, advised the committee that, although the Attorney-General's Department could not provide 'specific information' on the level and incidence of e-fraud against financial institutions, 'general threats to anybody on the internet, whether that is a user…or a company, are increasing.'[69]

7.84 Mr William Boulton, Examiner, Australian Crime Commission, explained that, despite online fraud being a fairly recent development, it is generally true that it is a 'very big growth area', and that the extent of this class of fraud is 'probably much greater than people realise'.[70]

7.85 Although banks and financial institutions have traditionally absorbed fraud-related losses, online vulnerabilities are generally ascribable to 'the interaction between the user and their computer and the bank'.[71] The committee is concerned that, if financial institutions decide in future to adopt a fault-based or stricter approach to apportioning liability for online losses, the cost to consumers will be significant.

7.86 The committee heard some evidence that banks are already passing online fraud related losses onto consumers.[72] Such claims raise important issues around accountability and the question of who is bearing, and who should bear, the burden of risk in cases of online fraud. This is particularly so if it is true that, as the submission from Mr Stephen Palleras QC, Director of Public Prosecutions for South Australia, asserts, most cases of online fraud are described as 'identity theft' or 'identity fraud' when in fact they are offences effected through entirely fictitious identities.[73] The lack of compulsory reporting of online crime means that banks could be passing on, or could in the future pass on, online crime costs to consumers based on a flawed description of an occurrence of fraud.

7.87 The committee was unable to secure the direct participation of the Australian High Tech Crime Centre (AHTCC), a body whose responsibility and expertise is directly related to such issues. Nevertheless, the committee was able to refer to the public comments of Mr Kevin Zuccato, the director of the AHTCC, on this subject.

7.88 On 24 June 2007, Mr Zuccato participated in ABC radio's *Background Briefing* story on the apparent vulnerability of the internet to high-tech crime and

[68] *Committee Hansard*, 5 July 2007, p. 90.

[69] *Committee Hansard*, 5 July 2007, p. 21.

[70] *Committee Hansard*, 6 July 2007, p. 47.

[71] Mr Alexander Webling, Senior Adviser E-Security Strategy, Critical Infrastructure Protection Branch, Attorney-General's Department, *Committee Hansard*, 5 July 2007, p. 21.

[72] Professor Rod Broadhurst, Private Capacity, *Committee Hansard*, 7 June 2007, p. 69.

[73] *Submission 6*, p. 1.

fraud. A major theme of the story was the claim that the true level of internet crime is under-reported because banks fear the negative consequences of consumers knowing bank security has been compromised. The internet, it was reported, has delivered massive profits to banks through new business models; they therefore prefer to absorb losses from fraud rather than publicise their own failings and potentially damage their reputation.[74] Mr McCusker also suggested that financial institutions are sensitive about the reputational risks of publicising such data.[75]

7.89 Professor Broadhurst agreed that reporting of fraud is a 'sensitive area' and that banks are reluctant to report and thereby advertise instances of fraud perpetrated against them for fear it will damage their reputation.[76] However, he believed there is a danger that an approach premised on a false sense of security could ultimately see the problem worsen:

> …if we let the mantra become, 'We need to look like everything is fine…we are running the risk of actually being run over.[77]

7.90 However, Mr Zuccato told *Background Briefing* that, despite 'hundreds of millions of dollars being defrauded', systematic disclosure of incidents of fraud is not useful for the average consumer, because it does not enable or help people to understand that there are risks associated with the use of the online environment:

> You and I don't really need to know the extent of the crimes, the hundreds of millions of dollars being defrauded, because it doesn't help…Speaking of how much is being lost doesn't really take us anywhere in relation to explaining to people that there is a risk.[78]

7.91 Further, Mr Zuccato considered that privacy issues prevent the publicising of data on the incidence of online fraud:

> …it would be remiss of us to publicise victims' names. So we wouldn't do that. What we try and do is basically understand what's happening, work with people to try and understand the level of the problem and then send the right messages to people so that they can take the appropriate action.[79]

7.92 However, this position was not supported by Professor Broadhurst, who argued that the vulnerability of the internet to fraud requires a balance to be struck between allowing the productivity and commercial benefits of the internet and ensuring that the system is sufficiently protected against criminal misuse:

> I think there is a balance. We do not want to overregulate the internet market. It is a hugely important market. It is growing so fast. It is going to

[74] ABC Radio, 'Your money dot con', *Background Briefing*, 24 June 2007, transcript, p. 2.

[75] *Committee Hansard*, 5 July 2007, p. 90.

[76] *Committee Hansard*, 7 June 2007, p. 69.

[77] *Committee Hansard*, 7 June 2007, p. 69.

[78] ABC Radio, 'Your money dot con', *Background Briefing*, 24 June 2007, transcript, p. 17.

[79] ABC Radio, 'Your money dot con', *Background Briefing*, 24 June 2007, transcript, p. 17.

> provide huge energy for productivity et cetera. But, of course, it is a superhighway that does not have many patrol cars on it, and a lot of the vehicles—the PCs and so on—that we use to drive on it do not have the appropriate safety equipment, if I can use that analogy.[80]

7.93 Mr McCusker observed:

> The corollary of [a reluctance to report online fraud]…of course, is that law enforcement cannot effectively fight this type of fraud and this kind of online activity unless they are made aware.[81]

Initiatives for the reporting and prevention of online fraud

7.94 The committee heard that, despite the apparent lack of compulsory reporting of online fraud, there are moves afoot to furnish relevant police agencies with data on the incidence of such offences. Mr Webling explained:

> The government has taken a very holistic view…in that it is trying to work with both the banks, as the owners of large systems which are on the internet, and with the users, as in you and me on the internet, and also small and medium enterprises.[82]

7.95 Dr Dianne Heriot, Acting First Assistant Secretary, Criminal Justice Division, Attorney-General’s Department, observed that the current approach to reporting online fraud offences is a collaborative one based on 'government-industry engagement at an operational and policy level around the range of the issues'.[83]

7.96 Dr Makkai described the AIC's plans, following a specific-purpose grant drawn from the proceeds of crime, for a survey that will rectify some of the present gaps in knowledge:

> In order to improve our understanding of high-tech crime, the institute recently received funds from the proceeds of crime to examine the extent and impact of computer security incidents across all Australian industry sectors. This will be the first random survey of this scale and depth in Australia. We have completed our pilot and are now proceeding to conduct the main survey, which will be of approximately 20,000 businesses, but it will be another year before that is finalised and completed and ready for release.[84]

7.97 The committee notes that the ACC is collecting information on banking fraud, following the establishment of protocols or working arrangements that address the commercial concerns of banks. The ACC is able to compel the provision of such

[80] *Committee Hansard*, 7 June 2007, p. 69.

[81] *Committee Hansard*, 5 July 2007, p. 90.

[82] *Committee Hansard*, 5 July 2007, p. 21.

[83] *Committee Hansard*, 5 July 2007, p. 21.

[84] *Committee Hansard*, 5 July 2007, p. 85.

information, overcoming the lack of explicit reporting requirements on banks and financial institutions. Mr Boulton told the committee:

> …in the last few months the examiners have issued a number of notices to banks, insurance companies and the like, seeking under compulsion…instances of fraud perpetrated against those bodies. We are getting a lot of information coming back. The banks and insurance companies like this method because, even though it is compulsory, it is also confidential. We see that as a very big growth area…The extent of it is probably much greater than people realise.[85]

7.98 Mr Jeff Pope, General Manager, Commodities, Methodologies and Activities, ACC, outlined the recent process of collecting data on online fraud, and its high value to the ACC's investigations into, and assessments of, organised crime:

> …we have formed some very productive relationships with financial institution and…issued numerous notices in cooperation with these institutions. As a result…we have access…to over 200,000 [anonymous] data sets that are previously unreported incidents of fraud committed against those organisations. When added to our current intelligence holdings and systems this significantly enhances our ability to gain an understanding of individuals' criminal activities, serious and organised crime groups' presence in the financial sectors…and…diversification of their activities and, essentially, footprints of organised crime in areas that were previously either undetected or that we only had anecdotal evidence of. We are finding it to be a very powerful and successful way in which we can value-add to our intelligence holdings, but more importantly our understanding of organised crime in that area.[86]

7.99 The committee believes that the area of online banking fraud is expanding and will continue to at a significant rate. This growth will in part be due to the increasing numbers of consumers taking up and using this form of banking and the greater opportunities for criminal groups and individuals to engage in fraudulent activities in a relatively risk-free environment. While the committee appreciates that it is arguably not in the banks' best interests to publicly report online fraud, it is ultimately consumers who are required to pay for the rectification of this problem. Therefore banking consumers should be made fully aware of the potential associated risks.

Recommendation 16

7.100 The committee recommends that the Commonwealth Government seek to ensure the comprehensive and public reporting of online fraud, particularly within the banking and finance industry.

[85] *Committee Hansard*, 6 July 2007, p. 47.

[86] *Committee Hansard*, 6 July 2007, p. 48.

Conclusion

7.101 The inquiry has identified a range of administrative and regulatory practices that undermine current efforts to address serious and organised crime. Weaknesses were found in the area of telecommunications, particularly in the inaccurate registration of mobile phone SIM card users and the ability of VoIP to obscure the identity of its users.

7.102 The committee is concerned about the apparent instability of staffing in Australia's police forces and the loss of skilled sworn personnel to the private sector. There appears to be an opportunity for all jurisdictions to take a more coordinated and collaborative approach to the recruitment and retention of skilled personnel.

7.103 This chapter also highlighted the need for a sound research and evaluation base in addressing organised crime. The committee is concerned that online fraud is greatly under-reported, which appears to contradict principles of transparency and compulsory reporting of crime that are well accepted in other areas of the law and policing. If LEAs do not have a clear picture of the extent of online banking fraud then their task of policing such activities is rendered more difficult. Equally, if banking consumers are not advised as to the full extent of risk around online services they are unable to make adequately informed assessments and choices about which services and technologies to use. The committee notes that informed consumer choice is often a powerful driver for companies to improve or make more secure their products and services.

7.104 Ultimately, the committee is concerned to ensure that LEAs, regardless of jurisdiction, are well supported and equipped to tackle serious and organised crime. By addressing the administrative weaknesses identified, the committee hopes that LEAs will be assisted and made more effective in their fight against serious and organised crime.

7.105 The following chapter examines the adequacy of current databases and suggests potential areas of improvement.