SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 108

Senator Carr asked the following question at the hearing on 24 May 2005:

How many convictions have there been in those investigations?

The answer to the honourable senator's question is as follows:

There has been one conviction.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 109

Senator Carr asked the following question at the hearing on 24 May 2005:

In the last five years, how many raids have there been on a newspaper office for investigations in regard to an unauthorised disclosure?

The answer to the honourable senator's question is as follows:

In the last five years, there have been two search warrants executed on the offices of newspapers in relation to unauthorised disclosures.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 110

Senator Carr asked the following question at the hearing on 24 May 2005:

Investigation into the Department of Veterans' Affairs cabinet document – how long has it been before the court?

The answer to the honourable senator's question is as follows:

The defendant was summonsed to appear before the Melbourne Magistrates Court on 23 September 2004.

On 30 November 2004 he was committed for trial in the Melbourne Magistrates Court and entered into County Court Bail.

The matter is set down for trial on 8 July 2005.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 111

Senator Ludwig asked the following question at the hearing on 24 May 2005:

Counter terrorism Regional Engagement Teams – mentioned four other regional neighbours. Are you able to identify them to the Committee?

The answer to the honourable senator's question is as follows:

The Australian Federal Police (AFP) is undertaking feasibility studies to determine the need and demand for an AFP presence in four countries, namely Bangladesh, Laos, India and Sri Lanka. This includes liaising with host country agencies and scoping the counter terrorism and criminal environment in those countries.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 112

Senator Ludwig asked the following question at the hearing on 24 May 2005:

'Fighting Terrorism at its Source'

a) What are the exact funding figures that are allocated to programs out of the PBS and how they aggregate to the final figure?

b) Break it down into what is coming out of your own budget and what is new money which is then for specific outcomes? (Please note on the bottom how the different programs might interact)

The answer to the honourable senator's question is as follows:

a) The new policy initiative *Fighting Terrorism at its Source*, was included as a measure in the AFP's 2004-2005 Portfolio Additional Estimates Statement:

- 2004/05 – $9.935m (expense) and $6.38 m (capital)
- 2005/06 – $21.275m (expense)
- 2006/07 - $21.496m (expense)
- 2007-08 - $21.719m (expense)

The above appropriation provides additional resources for a number of AFP functions, including specifically regional cooperation teams, enhancing intelligence and surveillance capacity, language training and capacity building projects.

b) There was no breakdown of the *Fighting Terrorism at its Source* initiative in the Portfolio Budget Statement for 2005/06.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 113

Senator Ludwig asked the following question at the hearing on 24 May 2005:

Counter terrorism surveillance teams, intelligence officers and other specialists and the regional engagement team –

a) Are any officers currently being deployed?

b) If so, what is the number of officers being deployed in those roles?

c) Is there any intention to employ further officers?

The answer to the honourable senator's question is as follows:

a) Two Counter Terrorism Regional Cooperation Teams are currently deployed offshore. Surveillance and intelligence teams are domestic based with enhanced capacity for regional counterparts being achieved through training and provision of equipment under this policy initiative.

b) Deployments under this initiative currently comprise:

- 9 in the bilateral team in the Philippines
- 3 in the multi-national team in Indonesia
- 4 for the feasibility studies

These teams complement the team of 10 in Indonesia, which is not funded under this initiative.

The core teams based in the Philippines and Indonesia comprise investigative (counter terrorism, high tech crime and financial), intelligence, analytical and operational support. Additional technical and specialist personnel have deployed from time to time to provide specialist support to all teams.

Team numbers and expertise fluctuates depending on the operating environment and needs and requests of the host agency.

c) The AFP has established dialogue with other regional partners regarding capacity for the AFP to work collaboratively on counter terrorism matters. There is no intention to deploy anywhere else in the region at present. Deployments – whether they are under this initiative or under the counter terrorism rapid response initiative – are subject to a request and agreement from regional counterparts.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 114

Senator Ludwig asked the following question at the hearing on 24 May 2005:

National Missing Persons Unit –

a) how many calls does it receive.

b) is there a breakdown of the number of calls received.

The answer to the honourable senator's question is as follows:

a) During the period 2003/04 approximately 481 calls were received on the hotline. During the period July 2004 to 16 May 2005, 1454 calls were received on the hotline. The NMPU receives an average of 20 calls per day outside of the 1800 number.

b) Calls are broken down into a number of categories such as State Police Enquiries, Sightings, Genealogy, Media and Enquiry Status. The number of calls for each category is not readily available.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 115

Senator Ludwig asked the following question at the hearing on 24 May 2005:

National Missing Persons Unit –

a) Since 2003 has there always been two officers employed there – one sworn and one unsworn?

b) If staffing levels have changed since the inception of the Unit please advise what those changes were.

The answer to the honourable senator's question is as follows:

a) Between 1 July and 10 November 2003 two unsworn members were deployed to the National Missing Persons Unit. Since November 2003 one sworn and one unsworn member have been deployed to the Unit.

b) There have been no changes in staffing levels since 2003.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 116

Senator Ludwig asked the following question at the hearing on 24 May 2005:

National Missing Persons Unit –

a) is the allocation of the funding effectively for the payment of staff and ancillary costs?

b) please break down the figures from 2003.

The answer to the honourable senator's question is as follows:

a) The budget allocation of $0.108m received by the AFP to support this responsibility in July 2003 lapsed in June 2004. This funding was for the payment of staff and associated expenses. The AFP funding of the NMPU for the financial year 2004/2005 is approximately $0.280m, an increase of over 200%**.** This is funded from the AFP core budget and is for payment of staff and associated operating expenses.

b) The actual expenditure for 2003/2004 financial year was $187,460.84 in employee expenses and $29,956.11 in supplier expenses. The actual year to date expenditure for the 2004/2005 financial year as at 31 May 2005 is $155,872 in employee expenses and $69,628 in supplier expenses.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 117

Senator Ludwig asked the following question at the hearing on 24 May 2005:

When did the National Advisory Committee and Police Consultative Group last meet?

The answer to the honourable senator's question is as follows:

The National Advisory Committee on Missing Persons and the Police Consultative Group on Missing Persons last met on 16 and 17 June 2005.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 118

Senator Ludwig asked the following question at the hearing on 24 May 2005:

What hours is the National Missing Persons Unit staffed?

The answer to the honourable senator's question is as follows:

The National Missing Persons Unit is staffed between 0800 and 1700 Monday to Friday.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN FEDERAL POLICE

Question No. 119

Senator Ludwig asked the following question at the hearing on 24 May 2005:

a) How much does it cost to run the National Missing Persons website?

b) How many hits or page impressions does it receive?

The answer to the honourable senator's question is as follows:

a) The National Missing Persons Unit website is maintained by AFP Web Administration and the associated cost is absorbed by the AFP. It is not possible to provide an estimate of this cost.

b) The current system does not enable a breakdown of hits or page impressions received by the National Missing Person Unit website. The AFP Web Administration is currently upgrading the capacity to capture this information.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN GOVERNMENT SOLICITOR

Question No. 120

Senator Ludwig asked the following question at the hearing on 24 May 2005:

Does AGS have expertise in space law? Please define 'space law'.

The answer to the honourable senator's question is as follows:

Space law might be broadly described as the legal and regulatory framework which governs the world's activities in relation to outer space. It encompasses a range of areas of legal practice including:

- statutory interpretation - eg the *Space Activities Act 1998*
- regulation - eg licensing arrangements for launch facilities
- commercial law - eg contracts and insurance and risk issues related to space activities
- litigation and dispute resolution - eg damage caused to persons or property by space objects
- international law - eg requirements under the various UN space and communications treaties to which Australia is a signatory.

AGS has a number of lawyers with experience and expertise in the various areas of legal practice as applied to space law.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN INSTITUTE OF CRIMINOLOGY

Question No. 121

Senator Ludwig asked the following question at the hearing on 24 May 2005:

Please provide copies of the Trends and Issues papers regarding online child pornography

The answer to the honourable senator's question is as follows:

The Institute has released two papers on this topic to date.

Please find attached copies of

- AIC *Trends and Issues* paper, no. 279 "A Typology of Online Child Pornography Offending"

- AIC *Trends and Issues* paper, no. 299 "Does Thinking Make It So? Defining Online Child Pornography Possession Offences"

TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 279 July 2004

A Typology of Online Child Pornography Offending

Tony Krone

The Internet has increased the range, volume and accessibility of sexually abusive imagery, including child pornography. Child pornography depicts the sexual or sexualised physical abuse of children under 16 years of age. Australia has joined many other nations in an international effort to combat this multi-faceted global menace that combines both heavily networked and highly individualised criminal behaviour. This paper examines the typology of online child pornography offending, as well as law enforcement responses to the problem. This work is a result of a collaborative program between the Australian Institute of Criminology and the Australian High Tech Crime Centre.

Toni Makkai
Acting Director

AUSTRALIAN HIGH TECH CRIME CENTRE

ISSN 0817-8542

ISBN 0 642 53843 3

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends & issues in crime and criminal justice series, visit the AIC web site at:http://www.aic.gov.au

Child pornography existed before the creation of the Internet. It is not possible to say whether the advent of the Internet has fuelled the demand for child pornography and expanded an existing market, or whether it simply satisfies in new ways a market that would have existed in any event. It is clear, though, that the Internet provides an environment for the proliferation of child pornography and the creation of an expanding market for its consumption. This paper explores three important questions:

- What is online child pornography?
- Is there a typology of offending online?
- If so, what are the implications for law enforcement?

What is child pornography? A non-legal definition

As pointed out by Taylor and Quayle (2003), the legal definition of child pornography does not capture all the material that an adult with a sexual interest in children may consider sexualised or sexual. As they argue, understanding why child pornography is produced and collected requires us to think beyond the legal definition of child pornography. Based on a study of online content at the Combating Paedophile Information Networks in Europe centre (COPINE), Taylor and Quayle identified 10 categories of pictures that may be sexualised by an adult with a sexual interest in children. Material in some of these categories does not come within the legal definition of child pornography. For example, in the first category are non-erotic and non-sexualised pictures of children in their underwear or swimming costumes from commercial or private sources, in which the context or organisation by the collector indicates inappropriateness. The second category comprises pictures of naked or semi-naked children in appropriate nudist settings. The third category is of surreptitiously taken photographs of children in play areas or other safe environments showing underwear or varying degrees of nakedness.

Although material in the first category and some of the material in the second and third will not be caught by the legal definition of child pornography, all may be indicative of a sexual interest in children and are therefore potentially important in the investigation of child pornography offences.

The legal definition of child pornography

The Australian regime to regulate pornography (whether online or not) essentially relies on state and territory laws (for convenience referred to here as 'state laws'). The provisions prohibiting the possession of child pornography are listed in Table 1. There are also provisions against the manufacture, distribution or sale of child pornography with more severe penalties.

Child pornography is generally defined as material that describes or depicts a person under 16 years of age, or who appears to be less than 16, in a manner that would offend a reasonable adult. However, this legal definition can be difficult to apply (Grant et al. 1997) because of jurisdictional differences. For example, in some states there must also be the depiction of sexual activity by the child or some other person in the presence of the child. Difficulty also arises from the fact that child pornography laws usually require a judgment to be made whether material is offensive or not.

The state laws regarding child pornography intersect with federal censorship laws contained in the *Classification (Publications, Films and Computer Games) Act 1995* (Cwlth). In two jurisdictions (NSW and NT) the legal definition of child pornography also includes material that has been refused classification under this Classification Act.

The *Broadcasting Services Amendment (Online Services) Act 1999* (Cwlth) created a non-criminal process for reporting web sites that host material which would be refused classification (as well as X- and R-rated material that is easily accessible without adult verification). The Australian Broadcasting Authority (ABA) can issue a take-down notice to have Australian-based web sites remove this content. If the site is hosted overseas, the ABA can notify content filter developers to add it to their lists of offensive sites (Chalmers 2002).

Proposed national law

In June 2004 the Australian government introduced a Bill to enact federal laws, tied to the power to regulate telecommunications, covering child pornography and grooming (Attorney-General's Department 2004). The Bill defines child pornography in terms of the depiction of a child under 18 years of age and provides for a penalty of 10 years for possession of child pornography, and 15 years for online grooming.

Children actually or apparently under 16

It is not necessary to prove that a child depicted was in fact less than 16 years of age at the time the image was created. It is enough that they appear to be under that age. The legislation therefore applies to images of a person over the age of 16 who is made to appear younger than that. Standard medical indicators of the physical developmental stages of children may be used to assess whether an image depicts a child under the age of 16 (Censorship Review Board 2000).

Table 1: Child pornography possession offences

Jurisdiction	Provision	Year	Maximum penalty
ACT	s 65, *Crimes Act 1900*	1991	5 years
NSW	s 578B, *Crimes Act 1900*	1995	2 years/100 penalty units
NT	s 125B, *Criminal Code*	1996	2 years/$20,000 corporate penalty
Qld	s 14, *Classification of Publications Act 1991*	1991	1 year/300 penalty units
SA	s 33, *Summary Offences Act 1953*	1992	1 year/$5,000
Tas.	s 74, *Classification (Publications, Films and Computer Games) Enforcement Act 1995*	1995	1 year/50 penalty units
Vic.	s 70, *Crimes Act 1958*	1995	10 years
WA	s 60, *Censorship Act 1996*	1996	5 years

Morphed images of children

The definition of child pornography may include morphed pictures. Taylor (1999) refers to such images as pseudo-photographs, and they are classified according to three types:

- digitally altered and sexualised images of bodies, such as a photograph of a child in a swimming costume where the costume has been electronically removed;
- separate images in one picture, such as a child's hand superimposed onto an adult penis; and
- a montage of pictures, some of which are sexual.

The ease with which a morphed collection can be put together, even without the capacity to digitally alter images, is illustrated by the case of convicted double murderer and serial rapist Lenny Lawson. Lawson was one of Australia's longest serving prisoners when he died in custody at the age of 76, three days after being transferred to a maximum-security unit. This transfer followed the discovery in Lawson's cell of a collection of video tapes which in part contained images from *Sesame Street* spliced with other program material to produce what was described by the prison psychologist as a collection of 'voyeuristic sexual fantasies and sexual perversion, often associated with children' (Mitchell 2004).

Creating fictitious children under 16

Child pornography can be created without directly involving a real person. The words 'describing or depicting' are capable of including text, images and three-dimensional objects. While these laws were initially framed in relation to photographs, videos and film, the language extends to cover the development of online pornography. The offence provisions do not require a real person to be described or depicted, and they include fictional characters in text or digitally created images of fictional characters.

In *Dodge v R* (2002) A Crim R 435, a prisoner in Western Australia who was serving a long sentence for sexual offences against children was convicted of further offences after writing 17 sexually explicit stories about adult males involved in

Table 2: Categories of child pornography

Level	Description	COPINE typology
1	Images depicting nudity or erotic posing, with no sexual activity	Nudist (naked or semi-naked in legitimate settings/ sources); Erotica (surreptitious photographs showing underwear/nakedness); Posing (deliberate posing suggesting sexual content); and Explicit erotic posing (emphasis on genital area)
2	Sexual activity between children, or solo masturbation by a child	Explicit sexual activity not involving an adult
3	Non-penetrative sexual activity between adult(s) and child(ren)	Assault (sexual assault involving an adult)
4	Penetrative sexual activity between adult(s) and child(ren)	Gross assault (penetrative assault involving an adult)
5	Sadism or bestiality	Sadistic/bestiality (sexual images involving pain or animals)

Source: Sentencing Advisory Panel 2002

sexual acts with young children (mostly boys aged less than 10). Dodge pleaded guilty to child pornography charges for supplying another prisoner with these stories and of possessing the stories himself. The appeal court noted that a prison sentence was required because the law sought to prevent access to child pornography. However, the fact that no child was involved in producing the material was taken into account in reducing the sentence from 18 to 12 months.

In contrast to the law in Australia, the United States' *Child Pornography Prevention Act 1996* was a federal law that sought to prohibit virtual child pornography. However the relevant provision was struck down for being too widely drafted. In *Ashcroft v Free Speech Coalition* (00-795) 535 US 234 (2002) the United States Supreme Court held that the section infringed the First Amendment right to free speech. The provision defined child pornography widely using the words 'appears to be' and 'conveys the impression' in relation to depicting a person under the age of 18. The Court found this wording too broad in the absence of any requirement in the same provision for the prosecution to prove that the material is obscene.

Artistic merit or scientific or other purpose

The question of artistic merit must be considered in relation to whether material is offensive to a reasonable adult person or not. In South Australia, a work of artistic merit is exempted if there is not undue emphasis on its indecent or offensive aspects.

Material may not be classed as child pornography if it is held in good faith for the advancement or dissemination of legal, medical or scientific knowledge.

Possession for law enforcement purposes

Where not specifically exempted in the same legislative package, law enforcement officers rely on general powers of investigation and for the keeping of evidentiary material to retain child pornography for law enforcement purposes. Child pornography laws in NSW, Victoria, WA and NT allow a law enforcement officer to possess child pornography in the exercise or performance of a power, function or duty imposed by or under any Act or law.

Categorising child pornography

Police often distinguish between five categories of child pornographic images. The categories were originally developed in the United Kingdom based on the 10-point typology of such images developed by COPINE. These range from nudist shots and surreptitious eroticised underwear or semi-naked shots, through to penetrative sexual assault and sadism or bestiality (Table 2). While it may be beneficial for police to prioritise their investigations by reference to the seriousness of the images involved, the full extent of an offender's collection may not be known until an investigation is well under way.

As indicated above, not all material in the categories of nudist or erotica would fit the legal definition of child pornography. The courts must consider the context surrounding the making or keeping of material in deciding whether it is child pornography or not.

When it comes to assessing the severity of an offence of possessing child pornography, it is not enough to measure the number of images of various types involved. There are other indicators of seriousness, such as the offender's engagement with the material. This may include how long it has been held, the degree to which it is organised by the offender, how it was acquired, and whether it is a trophy of the offender's own sexual abuse of a child (Taylor & Quayle 2003).

How are offences committed online? A typology of offending

As noted by Taylor and Quayle (2003), the Internet provides the social, individual and technological circumstances in which an interest in child pornography flourishes.

- *Social*
  The Internet has been used to create a self-justifying online community for child pornography users.
- *Individual*
  Using the Internet, individuals can access material and communicate with others through a computer terminal providing an apparently private sphere for the expression of sexual fantasy.
- *Technological*
  Digital technology and the Internet make it possible for child pornography consumers to become obsessive collectors so that the collection of images becomes an end in itself. The Internet also provides a ready means to access material supporting increasingly extreme sexual fantasies. It can then be used to act out those fantasies with children in online interactions or in physical meetings arranged online.

Knowing the differences in how online child pornography offences are committed is vitally important to understanding and combating the problem of sexual exploitation of children. What follows is a

discussion of the typology of offending (summarised in Table 3). There is an increasing seriousness of offending, from offences that do not directly involve a child, to offences that involve direct contact with children, and from online grooming to physical abuse.

Browser

A browser may come across child pornography unintentionally (for example via spam) but then decide to keep it. This is an offence if it can be proved they formed the intention to possess the material. In the absence of a confession, this may be shown by surrounding circumstances, such as repeat visits to a site. Whether a person is an accidental browser or not is a question of fact.

Private fantasy

If a person has a private fantasy involving sex with a child, no offence is committed. If that fantasy is preserved as something more than a thought, then an offence may be involved. The representation of that fantasy in text or digital format on a computer may be sufficient to constitute the possession of child pornography even if the offender has no intention of sharing it with any other person. The case of Lenny Lawson, referred to above, is an example of a private fantasy collection in video format.

For the offender engaged in private fantasy the risk of exposure is low, but it could occur in a number of ways: by tip-off from someone else with access to the computer or data storage device; in the course of searching a computer for evidence of other offences; when a computer is being serviced; when a computer is stolen; or even when a computer has been accessed remotely by a third party.

Trawler

Among trawlers there is little or no security employed and minimal networking of offenders. Taylor (1999) lists three motivations. The sexually omnivorous user is oriented to a range of sexually explicit material of which child pornography is simply a part but not the focus. The sexually curious user has experimented with child pornographic material but has not pursued it. The libertarian is driven to assert a claim to be free to access whatever material they wish.

Non-secure collector

The non-secure collector purchases, downloads or exchanges child pornography from openly available sources on the Internet or in chat rooms that do not impose security barriers. Security barriers include passwords, encryption or the requirement to trade a minimum number of images. There is a higher degree of networking among non-secure collectors than among trawlers.

Secure collector

In contrast, the secure collector uses security barriers to collect pornography. In addition to encryption, some groups have an entry requirement that locks its members into protecting each other—each member is required to submit child pornography images to join. The W0nderland [sic] Club was one such international child pornography ring exposed in 1998. In order to join, members had to submit 10,000 child pornography images. Both open and private collectors may be driven by the desire to amass a

Table 3: A typology of online child pornography offending

Type of involvement	Features	Level of networking by offender	Security	Nature of abuse
Browser	Response to spam, accidental hit on suspect site—material knowingly saved	Nil	Nil	Indirect
Private fantasy	Conscious creation of online text or digital images for private use	Nil	Nil	Indirect
Trawler	Actively seeking child pornography using openly available browsers	Low	Nil	Indirect
Non-secure collector	Actively seeking material often through peer-to-peer networks	High	Nil	Indirect
Secure collector	Actively seeking material but only through secure networks. Collector syndrome and exchange as an entry barrier	High	Secure	Indirect
Groomer	Cultivating an online relationship with one or more children. The offender may or may not seek material in any of the above ways. Pornography may be used to facilitate abuse	Varies—online contact with individual children	Security depends on child	Direct
Physical abuser	Abusing a child who may have been introduced to the offender online. The offender may or may not seek material in any of the above ways. Pornography may be used to facilitate abuse	Varies—physical contact with individual children	Security depends on child	Direct
Producer	Records own abuse or that of others (or induces children to submit images of themselves)	Varies—may depend on whether becomes a distributor	Security depends on child	Direct
Distributor	May distribute at any one of the above levels	Varies	Tends to be secure	Indirect

collection. As a result, extremely large numbers of images can be involved.

In a WA case, *R v Jones* [1999] WASCA 24, the court considered the size of a collection as an aggravating feature on sentencing: 'the degradation of the children is more serious because there is a larger number of images involved.' The defendant had 162,000 images on a CD-ROM. The appeal court took into account both the number of children involved and the number of images of each child as aggravating features. The original two-year suspended sentence was replaced with a gaol term of 18 months.

In an English case the offender, Andrew Tatum, was jailed for five years for possessing 495,000 indecent images of children. An indication of the obsessive nature of his collecting is that the images upon which his conviction was based counted for only about five per cent of his personal collection of more than 10 million pornographic images (The Age 2004).

Online groomer

The online groomer is a person who has initiated online contact with a child with the intention of establishing a sexual relationship involving cyber sex or physical sex. Child pornography is used to 'groom' the child—it is shown to the child to lower that child's inhibitions concerning sexual activity. The proposed Commonwealth law referred to above covers indecent material as well as pornographic pictures and text when communicated to a child for the purpose of making it easier to procure that child for sexual activity, or to make it more likely that the child will engage in sexual activity (Attorney-General's Department 2004). The same proposed law includes specific offences of procuring a child for sexual purposes and refers to sending communications with the intent of facilitating a meeting as a precursor to sexual activity.

The current Queensland legislation contains an anti-grooming provision. The first successful prosecution under this law led to the sentencing of an offender to nine months imprisonment in February 2004. The 26-year-old had tried to procure a 13-year-old girl for sex using an Internet chat room. The 'girl' was in fact a police officer involved in a sting operation (Townsend 2004). Western Australia is developing similar legislation (Gallop 2004).

Physical abuser

Physical abusers are actively involved in the abuse of children and use child pornography to supplement their sexual craving. The physical abuse may be recorded for the personal use of the abuser but is not intended to be further distributed. In cases of this type, a charge of making or possessing child pornography will usually be incidental to a charge for the physical abuse that has taken place.

Producer

The producer of child pornography is involved in the physical abuse of children. He or she provides images of that abuse to other users of child pornography.

Distributor

The distributor of child pornography may or may not have a sexual interest in child pornography. For example, the Western Australian case of *R v W* (2000) 27 SR (WA) 148 involved a child who was prosecuted for possessing child pornography with the intent to sell it. The offender had set up a web site offshore to make money from advertisers. The content of the web site included images and textual references to child pornography. The court held he was properly convicted.

Profiling offenders

To the categories listed above might be added the child user or the youthful user who pursues material reflecting their own level of sexual maturity or exposure by adults to child pornography. It has been reported that children under 10 who have been exposed to sexually exploitative material have themselves become users of it (including child pornography) and abusers of other children (Stanley et al. 2003).

Research in the United States shows that the typical person arrested for child pornography offences is a Caucasian male over the age of 26 years (Wolak et al. 2003). Little is known, however, about the characteristics of offenders in Australia. Even if there were consistent patterns of gender and age among offenders, it would be wrong to assume that offending fits a homogenous profile. The typology presented above shows that there are at least eight different ways of offending, with four of these having no direct contact with children, three involving either online or physical contact, and one where there may or may not be contact with children. There are also significant differences in the level of security applied and the degree of networking engaged in. More research is required to explore the ways in which these different types of offending are interlinked. The most important research issues to address are:

- How can victims be identified to prevent ongoing abuse or provide support in relation to past abuse?
- What effects are suffered by victims portrayed in child pornography?
- What is the extent of recidivism among child pornography offenders?
- What are the most effective ways of rehabilitating a child pornography offender?
- Does the use of child pornography follow a typical progress from the marginally pornographic to the most extreme images?
- Is there any causal link between use of child pornography and the physical abuse of children?

Implications for law enforcement

Police are devoting increasing attention and resources to combat child pornography and online sex offences. Investigations are necessarily complex and time consuming because they are often coordinated across jurisdictions, they involve networks of offenders using varying levels of security, and an individual offender must be linked to the misuse of a computer.

Perhaps the most important factor in law enforcement is the reliance on networks by many offenders. Concentrating on these linkages is likely to help address the problem of the proliferation of child pornography. Stopping the physical abuse of children requires an intensive investigation effort concentrating on finding new material and on cracking into the more secretive world of individual and networked producers.

Police may use stings to locate individual offenders. The greater long-term value in any sting operation may lie in exploding the view that the Internet is an anonymous domain in

which it is safe to offend. Such sting operations may need to operate on a number of levels to capture the various ways in which offences may be committed online.

- Police stings using false web sites target unsophisticated users (Cyberspace Research Unit 2003). By catching trawlers and deterring those who may be thinking of experimenting with child pornography, an admittedly low level of offending will be disrupted. The Australian High Tech Crime Centre has joined the Virtual Global Taskforce of police from the UK, US and Canada to run such sting operations and other coordinated activities (The Guardian 2003).
- Sting operations aimed at groomers are more finely targeted at those who represent a real threat in terms of contacting children and acting out their sexual impulses. Queensland police have been able to operate with an anti-grooming law in that state to locate and prosecute groomers. We do not know how prevalent grooming is, and stings of this type may rely on the police officer and the offender drawing on a 'shared fantasy' of the 'compliant and sexualised child' (Taylor & Quayle 2003).

Much more needs to be done to understand the problem of online child pornography. The literature on adults with a sexual interest in children 'fails to accommodate behaviour that relates to the new technologies' (Taylor & Quayle 2003). Not only does this failure impede the treatment of offenders, it also hampers the ability to prioritise matters for investigation and for prosecution. At this stage, we can speak of associations between risk factors and models of offending behaviour. Drawing on the work by Taylor and Quayle (2003), the following are markers of serious online offending:

- possessing new or recent images, extreme images, or images associated with text;
- participating in an online community of offenders;
- trading in images; and
- cataloguing of images.

Investigators need to consider the extent to which an offender found with child pornography may be involved in other levels of offending. The development of predictive indicators of involvement would therefore be an important advance in combating child pornography.

In the meantime, law enforcement agencies must prioritise their investigation efforts. A useful scale of priorities has been developed in the UK in response to the flood of cases from Operation Ore. The top priority is given to cases involving convicted paedophiles and those with access to children, such as teachers and social workers. The second priority is given to cases involving people in positions of authority, for example police and magistrates. The third is for suspects not involved with children.

Conclusion

There is no doubting the importance of combating online child pornography in order to protect children from abuse. More research is needed to properly understand the problem, to fully assess the nature and scale of offending, to identify and protect victims and, ultimately, to ensure that our approach is both effective and just.

Acknowledgment

This research was funded by the Australian High Tech Crime Centre (www.ahtcc.gov.au).

References

Attorney-General's Department 2004. Internet child sex offences Bill tabled. Canberra: Attorney-General's Department. www.ag.gov.au

Censorship Review Board 2000. Decision of 32nd meeting, 19–20 October 2000: Untitled computer image (young blonde male with hand on soccer ball). Surry Hills: Censorship Review Board

Chalmers R 2002. Regulating the net in Australia: Firing blanks or silver bullets? *Murdoch University electronic journal of law* vol 9 no 3. www.murdoch.edu.au/elaw/issues/v9n3/chalmers93_text.html

Cyberspace Research Unit 2003. Response to the National Crime Squad's announcement regarding the launch of Operation Pin. www.uclan.ac.uk/host/cru/docs/crupr18122003.doc

Gallop G 2004. Covert police team to hunt online predators. Press release, 21 June 2004. www.mediastatements.wa.gov.au

Grant A, David F & Grabosky P 1997. Child pornography in the digital age. In *Transnational organised crime* vol 3 no 4: 171–188

Mitchell A 2004. Inside the mind of a killer. Sydney: *The Sun Herald* 22 February 2004: 55

Sentencing Advisory Panel 2002. The panel's advice to the court of appeal on offences involving child pornography. London: Sentencing Advisory Panel

Stanley J & Kovacs K 2003. Child abuse and the Internet *Ninth Australasian Conference on Child Abuse and Neglect*. Sydney: 25 November 2003

Taylor M & Quayle E 2003. *Child pornography: an Internet crime*. Hove: Brunner-Routledge

Taylor M 1999. The nature and dimensions of child pornography on the Internet *Combating child pornography on the Internet* conference, Vienna. www.asem.org/Documents/aaconfvienna/pa_taylor.html

The Age 2004. Five years for UK man who downloaded child porn. Melbourne: *The Age* 3March 2004. www.theage.com.au/articles/2004/03/03/1078191360537.html

The Guardian 2003. Police sting targets Internet paedophiles. London: *The Guardian* 18 December 2003. www.guardian.co.uk/child/story/0,7369,1109589,00.html

Townsend I 2004. Qld Internet sex laws reveal disturbing extent of Internet predators. *AM*. ABC Radio 14 February 2004. www.abc.net.au/am/content/2004/s1045034.htm

Wolak J, Mitchell K & Finkelhor D 2003. *Internet sex crimes against minors: the response of law enforcement*. New Hampshire: National Center for Missing and Exploited Children

Dr Tony Krone is a research analyst at the Australian Institute of Criminology

General editor, Trends & issues in crime and criminal justice series: Dr Toni Makkai, Acting Director Australian Institute of Criminology GPO Box 2944 Canberra ACT 2601 Note: Trends & issues in crime and criminal justice are refereed papers

The AIC is a statutory body with a Board of Management comprised of federal, state and territory government representatives, administered under the *Criminology Research Act 1971*

TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 299 April 2005

Does Thinking Make It So? Defining Online Child Pornography Possession Offences

Tony Krone

Investigations into the widespread possession of online child sexual abuse images reveal enormous variety in the types of images collected by adults with a sexual interest in children. While there is almost universal condemnation of the sexual exploitation of children through such images, it is not possible to define precisely what constitutes an illegal child sexual abuse image. This is because the concept is broad, changeable and, at the margins, elusive. Nonetheless, the use of criminal law to regulate any activity requires that the proscribed conduct be clearly defined. This paper reviews the ways in which child sexual abuse images can be categorised and, in particular, examines the impact of the viewer's perception on the definition of child pornography offences in Australia.

Toni Makkai
Director

AUSTRALIAN HIGH TECH CRIME CENTRE

ISSN 0817-8542

ISBN 0 642 53877 8

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends & issues in crime and criminal justice series, visit the AIC web site at: http://www.aic.gov.au

Project no. 0074

Traditionally in Australia, anti-pornography laws have been concerned with the importation, display or distribution of obscene or offensive material, but not its possession (Fox 1967). Certain types of adult pornography are banned and cannot be produced, imported, sold or otherwise distributed. However, mere possession of any form of adult pornography is not an offence. In contrast, the possession of child pornography has been criminalised since the early 1990s. Since that time, the internet has developed into a platform for easily gaining access to images of child sexual abuse, and child pornography offences have emerged as a focus for public attention. It is often assumed that the definition of child pornography is unproblematic and that all forms of child pornography are equally harmful. In fact, the harm caused by child pornography is not well understood and there is a need for cautious application of the label 'child pornography' to avoid legislative over-reach. For example, it would be an unintended consequence for the law to be applied to the keeping, for non-sexual purposes, of family holiday snapshots of children in varying stages of undress playing on the beach. However, if those same images are kept by a person for the purpose of sexual gratification, the question arises whether that purpose can properly be taken into account, if at all, in the definition of child pornography.

Defining child pornography: sexually explicit, explicit and offensive, or overall offensive

The manufacture, distribution, possession and accessing of child pornography are each separate offences. There are three basic ways in which child pornography is defined in Australia ranging from:

1 a specific requirement of describing or depicting sexual body parts or sexual acts involving children or depicting children in an indecent manner or context; to

2 describing or depicting sexual body parts or sexual acts involving children in a manner that is offensive; to

3 a general test of 'describing or depicting a child in a manner that would offend a reasonable adult.'

In some states, the showing of sexual activity or of the genitalia of a child is not necessary for an image to be classed as child pornography. The tests of indecency and offensiveness allow for consideration of context in the way an image is made or the way in which an image is viewed. This gives rise to a complaint that the standard is difficult to define. There is a long history of contention regarding obscenity laws that rely on the imprecise standard of what may offend a reasonable adult. Trial by jury is often seen as a valuable protector from the over-reach of the law regarding what reasonable people would consider offensive. However, in relation to child pornography possession offences, where such a charge is dealt with summarily, the factual question of whether material is offensive or not is decided by a magistrate sitting alone.

1 Sexually explicit

In two jurisdictions, child pornography is narrowly defined in relation to:

- sexual activity;
- the sexual parts of a child; or
- the depiction of a child in an indecent sexual context.

ACT law bans the representation of the sexual parts of a child or sexual activity by or in the presence of a child. Victorian law bans describing or depicting a child engaged in sexual activity or depicting a child in an indecent sexual manner or context.

2 Sexually explicit and offensive

The Commonwealth law against accessing child pornography combines the depiction of sexual activity or sexual body parts with a test of offensiveness to a reasonable adult person. Similarly, recent legislative reform such as the *Crimes Amendment (Child Pornography) Act 2004* (NSW) adopt a definition based on a combined test of the depiction of sexual acts, or sexual body parts, or depiction of a child in a sexual context, where this is done in a way that is offensive to a reasonable adult person.

3 A general test of offensiveness

In those jurisdictions that apply a general test of offensiveness, this implies an objective standard of what a reasonable adult might think. This standard has to be interpreted and applied to the facts of a particular case by the court. Given the breadth of the definition of child pornography, the courts face an enormous range of factual situations concerning the nature and amount of potentially illegal material that offenders may be charged with possessing. In relation to the problem of defining child pornography, this paper discusses three issues:

- what the image depicts;
- the context in which the image was made or is kept; and
- the way in which a particular person views the image.

What the image depicts

Taylor and Quayle (2003) list ten categories of images that are used as part of the sexual repertoire of persons with a sexual interest in children. This list was developed for the Combating paedophile information networks in Europe (COPINE) centre. The COPINE taxonomy was developed principally from a psychological perspective to better understand the collecting behaviour of adults with a sexual interest in children. Given this perspective, the COPINE taxonomy is more extensive than the criminal law definition. The categories are shown in Table 1.

While the range of child sexual abuse images that may be captured under Australian anti-child pornography laws is broad, there are three distinct categories that may be involved:

- images of child sexual abuse offences;
- images of children in sexual poses; and
- images of children that are sexualised by the viewer.

Table 1: Categories of child pornography

COPINE no.	COPINE categories of material used by persons with a sexual interest in children	UK Court of Appeal child pornography severity rating
1	Indicative	
2	Nudist	
3	Erotica	
4	Posing	1
5	Erotic posing	
6	Explicit erotic posing	
7	Explicit sexual activity	2
8	Assault	3
9	Gross assault	4
10	Sadistic/bestiality	5

Source: Taylor & Quayle 2003; *R v Oliver* (2003) Crim LR 127

Box 1: The UK approach

The UK Sentencing Advisory Panel (SAP) gave advice to the UK Court of Appeal on the definition of child pornography and reduced the COPINE classifications to create five categories of child pornography for law enforcement purposes. These categories were seen by SAP to be of increasing seriousness (Sentencing Advisory Panel 2002). However, the notion of seriousness may not be so simple, as some offline child sexual abusers may only use erotica or posing images to fuel their offline offending, rather than using images of more extreme forms of abuse. Importantly, while SAP was prepared to include items in COPINE categories two and three, this was actually opposed by a major child protection advocacy group, the Children's Charities' Coalition for Internet Safety (CCIS), which consistently argued against the inclusion of material described as 'indicative', 'nudist' or 'erotica' (CCIS 2002a, 2002b).

The status of images was resolved in the UK in the Court of Appeal decision of *R v Oliver* (2003) Crim LR 127, where it was held that images in categories one, two and three of the COPINE classification do not fit the criminal definition of child pornography for the UK, which is based on a standard of 'indecency'. The reduced categories of child pornography for law enforcement developed by the UK Court of Appeal are shown in Table 1. Images in levels two to five of the UK Court of Appeal taxonomy can be linked to specific offences involving children. Some images in UK Court of Appeal category one may also be linked to criminal acts of indecency involving a child.

Images of child sexual abuse offences

In the states where the definition of child pornography is based on the sexual explicitness of the image, offending images are likely to portray child sexual assault offences. Where offensiveness is part of the definition of child pornography, the offensiveness to a reasonable adult of images of child sexual abuse can be readily inferred.

Under state and territory law the consent of the child is simply not an issue in relation to offences that specifically criminalise sexual activity between an adult and a child less than 16 years of age. Currently, state and territory child pornography laws apply to material that describes or depicts a person under 16 years of age, or who appears to be less than 16. The use of language such as 'describing or depicting a person who is or appears to be less than 16 years of age' is capable of including 'morphed' images (digitally altered images of real persons) and wholly simulated images, where these are made to look like children. However, morphed and simulated images are not the focus of this paper (see Krone 2004).

The maximum penalties provided for offline sexual assault offences with children are graded according to the age of the child involved and the degree of intrusiveness of the act involved. The most serious offence is sexual intercourse with a child, and this encompasses a range of sexually penetrative acts. The maximum penalty differs depending on which age band the child fits into at the time of the offence. Commonly, three age bands are used:

- less than 10 years of age;
- 10 years and above up to 14 years; and
- 14 years and above up to 16 years.

Similar age categories are commonly used to aggravate the penalty for less serious offences of indecent assault and committing an act of indecency with or towards a child. Considerations of youthfulness and degree of intrusiveness in any action depicted may be considered in defining child pornography and then rating its relative seriousness. The age of the child depicted may be important in applying a standard of offensiveness, given a greater abhorrence towards the sexualisation of the very young.

The *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No 2) 2004* (Cth) creates an offence of accessing child pornography and defines child pornography in terms of children under the age of 18 years, using a combined test of sexual explicitness and offensiveness. Given that the age of consent for sexual relations is generally 16 years for heterosexual and homosexual relations, there may be some difficulty in applying the same standards for child pornography in relation to a child under 16 (or more particularly under 10 years of age), to images of children between 16 and 18 years of age. It may be that a reasonable adult would consider the depiction of consensual sexual relations by a person with legal capacity to enter such relations as not being offensive when viewed in private by an adult. It may be thought to be offensive, however, if obtaining images involved a breach of privacy, or if the image depicted the commission of an offence of non-consensual sexual assault. Under existing state laws such invasive or violent images of persons over 16, but less than 18 years of age, are not captured by the definition of child pornography.

Images of children in sexual poses

Sexual poses are also likely to be offensive, particularly in relation to the involvement of younger children. In a general sense, images in COPINE categories four (posing), five (erotic posing, which involves sexualised or provocative poses) and six (explicit erotic posing, which has a deliberate emphasis on the genital region) may be considered to be child pornography and could well involve the portrayal of acts of indecency or aggravated acts of indecency. The deliberate sexual posing of children introduces an aspect of harm through the sexual exploitation of the child being photographed.

Images of children that are sexualised by the viewer

Other images of children are much less readily categorised as child pornography. Images in COPINE categories one (indicative material), two (nudist) and three (erotica) are unlikely to be considered offensive in Australia unless an aspect of their production or the manner in which they are kept introduces an additional element of indecency or offensiveness. In some instances, consideration of the context in which an image was obtained or is kept may be used to establish offensiveness.

The importance of context in the making of images

While a photograph of a partially clothed child, when viewed singly, may cause no concern to the objective viewer, what difference does it make if the images were taken surreptitiously without consent? Context may be a factor in assessing standards of indecency or offensiveness in the definition of child pornography, particularly in relation to collections of images of pre-pubescent children and collections of images of pre-school children. Images might be found to be offensive on the basis of the manner in which they were obtained, such as by intruding on the privacy of those photographed or by using force.

Another example where the context of the production of an image may cause it to be indecent or offensive to a reasonable adult viewer is where a child is photographed apparently in a state of unconsciousness or under the influence of a drug. This is a very menacing aspect of the manner in which some child pornography is produced and the apparently drug-affected appearance of child subjects in pornography has been noted (Taylor & Quayle 2003).

The viewer's gaze and the context in which images are kept

People may view the same image differently. The idea of the 'viewer's gaze' is that images of children that cannot be described as intrinsically offensive may become so because they are sexualised by the viewer. For example, an image of a child in underwear taken from a store catalogue may appear innocuous to one viewer and be highly sexualised for another. What then is the effect of a collection of many thousands of photographs of partially clothed children? What if those photographs are mixed in galleries with photographs of children being subjected to obvious sexual abuse or are used to illustrate written descriptions of the sexual abuse of children?

As indicated above, the criminalisation of the possession of child pornography represents a departure from previous approaches to content-related offences. Previously, tests of obscenity or offensiveness were evaluated in terms of the potential audience (Fox 1967). The essence of a possession charge is that an offender, for their own private use, keeps material without exposing it to a wider audience. Taking into account

Box 2: Case study

In *P v South Australia Police* (1994) 75 A Crim R 480, charges of possession of child pornography were laid in relation to four tapes running for 11 hours, of men and boys changing or urinating that were recorded in public toilets and change rooms. In some instances this included views of boys less than 16 years of age. The defendant had secretly recorded males at a number of venues in Adelaide and compiled the tapes. In a few instances a boy's penis could be seen, accounting for about 20 minutes of the total time on the tapes. On appeal, it was held in the Supreme Court that the then law required the court to ignore the circumstances of the making of the tape and, as a result, indecency could not be established based on the invasion of privacy inherent in compiling the tape. The court said that the section:

> [S]eems to have been drawn on the footing that there is material which is either inherently indecent or obscene. The proposition is, I think fallacious… It is not difficult to postulate that certain material might be indecent in some circumstances but not in others.

The court also held that the cumulative effect of the totality of the tape could not be relied on to establish indecency, as most images were not of children but of men. In the end, the defendant was acquitted on appeal. The law in South Australia was later changed to allow courts to take into account context when deciding whether material was indecent or not.

the way in which images are viewed by a particular person in determining indecency was affirmed in the UK in *R v Oliver*. The court held that, in deciding whether material is child pornography, regard could be had to whether the amount, context and organisation of images suggested a sexual interest. In rare instances, it may be that offensiveness can be established by considering the viewer's gaze.

The sexualisation of everyday images of pre-pubescent children is referred to as the 'paedophilic gaze' by Taylor & Quayle (2003). However, the sexualisation of images of children is not confined to 'paedophiles', in the sense of persons sexually interested in pre-pubescent children, and the term paedophilic gaze is not adopted in this paper. It should also be noted that the relationship between paedophilia and online child pornography offending is not simple or direct and requires careful examination that is beyond the scope of this paper.

Strong concerns have been expressed that increasing awareness of child pornography will lead to the sexualisation of all images of children because of a general social awareness that for some, almost any image of a child may become sexually charged. One example cited is that of a Calvin Klein advertisement that appeared in the United States, which depicted two young boys in their underwear jumping on a couch. Following a public outcry, the advertisement was withdrawn (Adler 2001). Despite the fact that some persons with a sexual interest in children may sexualise otherwise innocuous images, we should stop and question whether that is a matter for the application of the criminal law and, if it is, how that might properly be captured within the definition of child pornography.

A distinctive feature among some offenders who possess child pornography is the extent to which they keep their collections in well-ordered libraries of images (Taylor & Quayle 2003). Years of experience as an FBI investigator led Lanning (1992) to observe that offenders almost never destroy a collection. The following general characteristics of collecting among preferential child pornography offenders were noted by Klain et al. (2001), drawing on the work of Lanning (1992), Tate (1992) and Armagh et al. (1999):

- the collection is important to the offender who will spend a significant amount of time and money on it;
- collections grow as offenders feel their collection is not sufficient and there is more material to collect;
- collections are kept in a neat and orderly fashion, particularly using computers (Armagh et al. 1999);
- collections are a permanent fixture in an offender's life and will be moved or hidden if the offender believes they are under investigation;
- offenders almost never destroy a collection;
- offenders hide their collections in concealed spaces so that they have ready and secure access to them;
- offenders often share their collections with like-minded persons.

Conclusions

There are questions of degree in the definition of child pornography and offender involvement with child sexual abuse images. Increasingly severe penalties are proposed for the possession of child pornography and there can be no doubting the seriousness with which this offence is viewed. This makes it all the more important to be clear about what constitutes child pornography and about the nature of child sexual abuse images being dealt with in a particular case.

Images of children less than 16 years of age in the UK Court of Appeal categories two to five clearly depict criminal sexual assaults regardless of consent of the child involved, and the classification of such images as child pornography is unlikely to be seriously contested. Material from UK Court of Appeal category one is less clearly classified as child pornography, even though it may show an abnormal sexual interest in children. It is probable, however, that community standards are less tolerant of the sexualisation of the images of pre-pubescent children and would treat sexualised images of children with increasing seriousness depending on the age of the child depicted.

The use of a scale based on the type of sexual abuse depicted and the age of any child involved is one way of differentiating between offences. There is merit in reserving prosecutions for those cases involving images of actual sexual abuse, including sexual posing and explicit sexual posing, rather than other eroticised material. Even so, there will be some offenders who use less offensive images as part of a fantasy script of their own and who may pose a risk in terms of committing child sexual assault offences offline. The risk of a particular offender being involved in the offline sexual abuse of children is not necessarily related to the type of image viewed by that person (Taylor & Quayle 2003). More research is needed into the relationship between sexual fantasies fed by these materials and instances of the actual sexual abuse of children by those who have such fantasies.

With marginal images there is also scope to argue that the context in which the image was made or the manner in which images are kept can be taken into account in assessing whether material is child pornography. The limits of such an approach have yet to be determined.

In some instances it may be difficult to discern how an image was obtained. The use of a spy camera to film children in toilets and change rooms, such as in the South Australian case of P (see Box 2), is readily identified as involving a gross invasion of privacy and this may contribute to a finding that such images are offensive. The manner in which images are kept will usually be self-evident upon investigation. In those states where the definition of child pornography requires the image to portray sexual activity or the genitalia of children so as to be offensive, the size and organisation of collections of such images may be found offensive to a reasonable adult person. Where child pornography is defined in terms of offensiveness alone there is scope to argue that a collection of everyday images, such as in clothing store catalogues, may be offensive. However, while the sexualisation by the viewer of otherwise benign images of children may be objectionable and repugnant to many, caution should be exercised before criminalising the possession of such images based on simply what the viewer thinks.

Acknowledgment

The Australian High Tech Crime Centre funded this research.

References

Adler A 2001. The perverse law of child pornography. *Columbia law review* 101: 209–73

Armagh D, Battaglia N & Lanning K 1999. *Use of computers in the sexual exploitation of children*. Washington DC: US Department of Justice

Children's Charities' Coalition for Internet Safety 2002a. Letter to Sentencing Advisory Panel 8 April. http://www.nch.org.uk/itok/chis/Sentencing08042002.doc (accessed 10 January 2005)

——— 2002b. Letter to the Lord Chief Justice of England 27 August. http://www.nch.org.uk/itok/chis/SAPFinalLetter.doc (accessed 10 January 2005)

Fox RG 1967. *The concept of obscenity*. Melbourne: The Law Book Company

Klain E, Davies H & Hicks M 2001. *Child pornography: the criminal justice system response*. Washington DC: American Bar Association Center on Children and the Law

Krone T 2004. A typology of online child pornography offending. *Trends & issues in crime and criminal justice* no 279. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/tandi2/tandi279.html (accessed 10 January 2005)

Lanning K 1992. *Child molesters: A behavioral analysis*. Washington DC: National Center for Missing and Exploited Children

Sentencing Advisory Panel 2002. *Sentencing Advisory Panel's advice to the Court of Appeal on sentences involving child pornography*. London: Sentencing Advisory Panel

Tate T 1992. The child pornography industry: international trade in child sexual abuse. In C Itzen (ed) *Pornography: women, violence and civil liberties*. Oxford: Oxford University Press

Taylor M & Quayle E 2003. *Child pornography: an internet crime*. Hove: Brunner Routledge

Recent AIC publications

Back issues of the *Trends & issues in crime and criminal justice* series are available on the AIC web site at: www.aic.gov.au/publications/

No. 298 Crime victimisation in Australia: key findings of the 2004 International crime victimisation survey

No. 297 Crime in the Australian fishing industry: key issues

No. 296 International police operations against online child pornography

No. 295 Police shopfronts and reporting to police by retailers

No. 294 Spam: nuisance or menace, prevention or cure?

No. 293 Indigenous male offending and substance abuse

No. 292 Gender and serious fraud in Australia and New Zealand

No. 291 Prosecutorial decisions in adult sexual assault cases

No. 290 Patterns of antisocial behaviour from early to late adolescence

No. 289 Key findings from the Drug use careers of female offenders study

No. 288 Victim credibility in adult sexual assault cases

No. 287 The whole of government approach to crime prevention

No. 286 Criminal forfeiture and restriction-of-use orders in sentencing high tech offenders

No. 285 Impediments to the successful investigation of transnational high tech crime

No. 284 Current trends in the rehabilitation of juvenile offenders

No. 283 Understanding male domestic partner abusers

No. 282 The 'Teen Triple P' positive parenting program: a preliminary evaluation

No. 281 Risk assessment by mental health professionals and the prevention of future violent behaviour

Dr Tony Krone is a high tech crime research analyst in the Global, economic and electronic crime program at the Australian Institute of Criminology

General editor, Trends & issues in crime and criminal justice series:
Dr Toni Makkai, Director, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601
Note: Trends & issues in crime and criminal justice are peer reviewed

The AIC is a statutory body with a Board of Management comprising Australian, state and territory government representatives, administered under the *Criminology Research Act 1971*

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN INSTITUTE OF CRIMINOLOGY

Question No. 122

Senator Ludwig asked the following question at the hearing on 24 May 2005:

Australian Crime and Violence Prevention Awards:

a) How many applications were there?

b) Who applied?

c) Against what criteria are prizes awarded?

The answer to the honourable senator's question is as follows:

a) 89

b) Community Service Groups, Support Services, Schools, City Councils, Police and Police and Community Youth Clubs, State Government Departments and Indigenous organisations.

c) The criteria, as assessed by the Committee, is:
1. a) Whether the project has prevented or reduced violence of other types of crime; or
   b) Whether the project strongly indicates the capacity to prevent or reduce violence or other types of crime
2. How well is the success of the project measured?
3. How suitable is the project for copying elsewhere?
4. How lasting are the outcomes likely to be?
5. How innovative or otherwise special is the project?
6. How well does the project raise community awareness of the issue?

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN INSTITUTE OF CRIMINOLOGY

Question No. 123

Senator Ludwig asked the following question at the hearing on 24 May 2005:

Who are the Australian Crime and Violence Prevention Awards committee?

The answer to the honourable senator's questions is as follows:

- **Australian Government –** Dr Toni Makkai, Director, Australian Institute of Criminology (Chair)
- **NSW** Superintendent Mick Plotecki, NSW Police
- **VIC** Mr Mark McBurney, Executive Director, Office of Crime Prevention, Department of Justice
- **QLD** Mr Paul Friedman, Executive Director, Community Safety & Support Policy Unit, Department of Communities
- **SA** Mr James Armitage, Acting Manager, Crime Prevention Unit, Attorney-General's Department
- **TAS** Commissioner Richard McCreadie, Tasmania Police (represented by Ms Sandra Lovell)
- **WA** Mrs Pat Morris, Mayor, City of Gosnells
- **NT** Ms Cheryl McCoy*, Executive Director, Office of Crime Prevention, Department of Justice
- **ACT** Ms Lil Hays, Department of Justice and Community Safety

* Nominated but is awaiting official confirmation

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION

Question No. 124

Senator Greig asked the following question at the hearing on 24 May 2005:

Please provide a copy of the ASIO submission to the 'Parliamentary Joint Committee on ASIO inquiry into ASIO's public reporting of its activities'.

The answer to the honourable senator's question is as follows:

ASIO made two unclassified submissions to this inquiry and both are available on the web site of the Parliamentary Joint Committee on ASIO, ASIS and DSD. They are also attached for the Senator's reference.

Australian Security Intelligence Organisation

Submission to the
Parliamentary Joint Committee on ASIO

"An inquiry into the nature, scope and appropriateness of the way in which ASIO reports to the Australian public on its activities"

5 July 2000

Contents

"An inquiry into the nature, scope and appropriateness of the way in which ASIO reports to the Australian public on its activities"

Submission by ASIO

Introduction

About ASIO

ASIO is Australia's security service. Its functions are to:

- obtain, assess and communicate intelligence relating to, and provide advice on, threats to security
- provide protective security advice
- within Australia, obtain under warrant intelligence relating to the intentions, capabilities and actions of foreign powers

The Australian Security Intelligence Organisation Act 1979 defines security as protection from:

- espionage
- sabotage
- politically motivated violence (PMV)
- promotion of communal violence
- attacks on Australia's defence system
- acts of foreign interference

ASIO does not have executive powers to enforce measures of security; its role is the collection, analysis and dissemination of intelligence relevant to security. As such, ASIO provides security advice to other Commonwealth agencies, advice which is relevant to their functions.

About this submission

The purpose of this submission is to inform the committee of:

- the nature of ASIO's existing reporting to the Australian public on its activities
- a comparison with the public reporting of other agencies in Australia and overseas
- ASIO's future reporting plans

In preparing this submission the term 'public reporting' has been interpreted to include all activities which enable the public to receive information about ASIO's work.

Part of this submission will comprise publications put out by ASIO and other Australian and foreign services.

ASIO's approach

ASIO seeks to provide as much information to the public as possible, within the constraints of security and resources. As a security organisation, much of the detail of ASIO's activities cannot be made public.

ASIO Act

ASIO's work is governed by the *Australian Security Intelligence Organisation Act 1979*. The Act is, of course, publicly available. It spells out the Organisation's functions and powers and provides a legislative framework for its work. In particular, the Act spells out the detail of:

- the functions of the Organisation
- the ability of the Attorney-General to issue guidelines to the Director-General
- the requirement for the Director-General to obtain the authority of the Attorney-General to carry out special powers activities under warrant, and the necessity for the Director-General to report to the Attorney on completion of each warrant
- the conditions which apply to the making of security assessments
- the requirement for the Director-General to regularly brief the Leader of the Opposition
- the Parliamentary Joint Committee
- the requirement to produce an Annual Report to the Attorney-General and an unclassified Report to Parliament

However, like most legislation, the Act is not particularly useful to members of the public as a quick, easily readable guide.

Attorney-General's guidelines

More detailed guidance for some aspects of ASIO's work is found in the guidelines issued by the Attorney-General to the Director-General in relation to:

- **Collection of Intelligence** (issued 1992) which regulates ASIO's activities in carrying out its intelligence collection function. In particular, it specifies that the degree of intrusion of ASIO's investigative methods should be commensurate with the level of threat.
- **Politically Motivated Violence** (issued 1988) which regulates ASIO's activities in carrying out its function in relation to PMV.
- **Staffing** (issued 1989) which requires the Director-General to employ staff in terms which are consistent with the government's public sector employment principles.

These guidelines have been tabled in Parliament and are available to the public.

Annual Report

ASIO's annual report is structured to comply with the *Requirements for Annual Reports* issued by the Department of Prime Minister and Cabinet. It also addresses specific requirements applying to the annual reports of Australia's intelligence and security agencies.

ASIO produces two versions of its annual report. The first version is classified and contains an account of ASIO's performance during the previous 12 months, including sensitive reporting on security risks and investigative outcomes that cannot be released publicly. That report is provided to the Attorney-General, the Leader of the Opposition, and a small group of other government ministers and senior government officials. In particular, it provides performance information to the Secretaries Committee on National Security which reports to the National Security Committee of Cabinet.

An abridged version is then prepared for the Attorney-General to table in the Parliament, excluding all sensitive information in accordance with section 94 of the ASIO Act.

This declassified Report to Parliament provides similar information to the reports of other agencies although, because of security sensitivities, it is more limited in detail in relation to some operational aspects of ASIO's work. The report includes an overview of the security environment, discussion of trends (for example, changes in demand for Threat Assessments) and identifies, in broad terms, investigative and corporate priorities.

Capability enhancements, ASIO's role in the National Anti-Terrorist Plan and ASIO's protective security responsibilities are also discussed.

Other information contained in the Report to Parliament includes:

- the number of threat assessments issued each year
- the number of security assessments issued for the Department of Immigration and Multicultural Affairs and the Department of Foreign Affairs and Trade to assist their decisions on visa issue and the rights of residence
- the number of security assessments which resulted in recommendations against visa issue
- the number of adverse or qualified assessments not accepted by the Foreign Minister (for example, the 1996/97 Report to Parliament reported that an applicant who was the subject of an adverse assessment by ASIO was granted temporary entry on national interest grounds)
- the number of personnel security assessments for public servants requiring security clearances, including the number of appeals against adverse assessments to the Administrative Appeals Tribunal and the outcomes of those appeals
- the number of requests under the Archives Act for access to ASIO records more than 30 years old, together with the percentage that were finalised within the statutory requirement of 90 days
- information on ASIO's workplace diversity program, categories of employment, occupational health and safety, equal opportunity employment practices and SES profile
- 25 pages of financial statements for the reporting year, audited in accordance with the Australian National Audit Office Auditing Standards

Inspector-General of Intelligence and Security

ASIO's activities are also the subject of the report to Parliament by the Inspector-General of Intelligence and Security (the IGIS).

The Office of the Inspector-General was established in 1987. Its role with respect to ASIO is to ensure the Organisation acts legally and with propriety and complies with ministerial guidelines and directives.

The IGIS may enquire into matters concerning ASIO and investigate complaints about ASIO from the public. The office reports annually to Government, and provides an unclassified version of the report for parliamentary and public readers. The report contains a summary of selected complaints and the outcome of inquiries. The IGIS report usually attracts some media attention.

If it is in the public interest, other IGIS reports on specific issues or complaints may be tabled in the Parliament and sometimes published. One example related to the suggestion that ASIO was involved in the Hilton bombing in 1978.

Parliamentary Joint Committee on ASIO

From time to time, the Parliamentary Joint Committee on ASIO conducts inquiries into matters which have been referred to it by the Attorney-General:

- **"ASIO and the Archives Act"** (reported April 1992)
- **"ASIO and Security Assessments"** (reported March 1994)
- **"An Advisory Report on the ASIO Legislation Amendment Bill 1999"** (reported May 1999)

In addition to those inquiries, the Director-General has provided briefings to the committee on a range of subjects. During 1999 briefings were provided on 11 March and 6 December.

Senate Estimates

Since 1993 ASIO has appeared before the Senate Legal and Constitutional Legislation Committee ('Senate Estimates') which allows general questioning on aspects of ASIO's work by Members of Parliament. However, because of security considerations, questioning of ASIO has been more restrained than questioning of other agencies. In a public reporting context, the following aspects of Senate Estimates are relevant:

- the hearings are open to the public and recorded in Hansard
- questions from the committee can be taken on notice, and the replies become part of the Hansard record

Additionally, the Director-General can provide members of the committee with a private briefing on sensitive security matters which does not form part of the Hansard record.

Questions on Notice

ASIO is required to respond to Questions on Notice in the same manner as any other agency. The responses become part of the Hansard record.

Portfolio Budget Statements

Details of ASIO's proposed activities for the coming year, including financial expenditure, are provided in the Portfolio Budget Statements. These follow the standard

outcome/output reporting framework, but in comparison with other agencies ASIO's statements are less detailed, reflecting the classified nature of most of ASIO's work.

Other Parliamentary Business

Members of ASIO can also be called to give evidence before other Parliamentary committees. During 1999 and 2000, ASIO appeared before the following committees:

- **Senate Scrutiny of Bills Committee** – This committee invited the Attorney and officials to talk about the proposed amendments to the *Telecommunications (Interception) Act 1979*. The Director-General and Legal Adviser appeared before the committee with a senior official from the Attorney-General's Department. The Organisation also contributed to written submissions to the committee. These appearances and submissions were recorded in Hansard.

- **Legal and Constitutional Legislation Committee** – The same Bill was referred to this committee which took evidence from senior officials including the Director-General. Again, this appearance formed part of the public record.

- **Joint Standing Committee on Migration** – This committee conducted an inquiry into *Immigration Entry Requirements for the Olympics*. Two ASIO officers gave evidence to the committee. This evidence was given in camera as it provided detailed advice on security checking procedures for entry into Australia.

Media Policy

Since the late 1970s, ASIO has had a modified 'neither confirm nor deny' policy in relation to requests for information by the media. This followed a recommendation by Justice Hope in the report of the Royal Commission on Intelligence and Security 1977, that consideration should be given to the Director-General speaking in public about ASIO and its role.

In 1985 ASIO established the position of Media Liaison Officer (MLO). The MLO has a direct telephone line which is listed in the telephone directories of some of the state capital cities. This complements the 1800 toll free number for the ASIO Central Office switchboard which appears in every Australian telephone directory.

The MLO is responsible for:

- being the central point of contact for telephone inquiries from journalists and members of the public

- coordinating interview requests from members of the media

- supplying inquirers with publicly available information on ASIO, for example *ASIO Now* and *What's ASIO about?* (mentioned in more detail on page 11) or information from the Report to Parliament.

But ASIO does not make any public comment on sensitive national security matters such as:

- targeting of individuals and organisations
- operational methods
- liaison arrangements with other Australian and foreign intelligence and security agencies

The only exception to this is when it would be more detrimental to security to say nothing. This first occurred in 1985 when Director-General Alan Wrigley denied allegations of ASIO's involvement in the Hilton Hotel bombing. Other examples include:

- David Sadleir's 'doorstop' interview at Central Office in 1992 in which he denied allegations that a document circulating in the Macedonian community in Melbourne had originated within ASIO
- allegations by a South Australian Member of Parliament (Peter Lewis) that he had worked overseas for ASIO (1993)

Very few media releases are issued by ASIO. In 1993 a media release was issued in relation to Mr Lewis's allegations, but since then ASIO has only issued media releases in connection with the tabling of its Report to Parliament.

In recent years there have been a number of media interviews given by Directors-General. The most recent have been with *The Australian* (March 1999), *The Australian Financial Review* (July 1997 and April 1999), 'Lateline' (July 1999), the *Age* (1999), and Radio National's 'National Interest' (April 1999).

ASIO's publications

ASIO has a number of publications which are available to members of the public:

- **ASIO Now** (first published 1996, revised 2000) is a 16 page booklet which seeks to provide a plain English account of ASIO's role and functions. It is commonly used to respond to certain types of inquiries by members of the public, for example school students doing assignments, and as part of an information package for applicants for ASIO employment.
- **What is ASIO about?** (first published 1995, revised 1998) is a leaflet which provides a brief account of ASIO.
- The **Corporate Plan** has been publicly available since 1993. The current plan covers the period 1998–2002. In addition to information on ASIO's planned

outcomes and outputs, the Corporate Plan provides information on ASIO's mission, vision, values and the precepts of security.

ASIO's Protective Security section also makes a number of publications available:

- **Testing Security Products** (1994)
- **What's the SCEC?** (Security, Construction and Equipment Committee) (1995)
- **What's ASIO's Role in Protective Security?** (1998)

Web site

ASIO's web site was launched by the Attorney-General on 22 June 2000. It provides the most extensive consolidation of background information on ASIO ever made available. Importantly, it provides members of the public with 24 hour access to information about ASIO.

The web site has several main sections, which contain information about various aspects of the Organisation. Subjects of interest include:

- **About ASIO**
  - What is ASIO?
  - Mission, vision and values
  - Management and structure
  - ASIO and the Australian Intelligence Community
  - Accountability
    - Attorney-General, including the guidelines
    - Parliamentary Joint Committee
    - Inspector-General of Intelligence and Security
  - Significant events in ASIO's history
  - Directors-General of Security
  - ASIO's 50th Anniversary (1949-99)
  - ASIO Staff Association
  - Frequently asked questions
- **ASIO's work**
  - The security environment
  - Threat assessments

- Security Assessments
- Protective Security and T4
- Sydney 2000 Games

- **Publications**
  - Corporate Plan
  - Annual Report
  - Testing Security Products
  - Security Equipment Catalogue
- **Employment**
  - Eligibility
  - Current vacancies
  - Categories of employment
  - How to apply
  - Conditions of service
  - Application forms
- **ASIO contact information**

The web site incorporates links to other sites including the Attorney-General, Parliamentary Joint Committee, the Inspector-General of Intelligence of Security and other members of the Australian Intelligence Community.

Other aspects of ASIO's reporting

Public presentations about ASIO

From time to time ASIO officers make speeches at public functions or conferences. Since Justice Woodward first addressed the National Press Club in 1977, several other Directors-General have followed suit. The current Director-General has addressed a diverse range of groups, including:

- Burgman College at the ANU (1997)
- the Australian Institute of Professional Intelligence Officers conference - opening address (1997)
- the Australian Security Industry Association's annual security conference (1998)

- the Committee for Economic Development of Australia in Melbourne in 1997 and in Sydney in 1998
- the United Services Institution of the ACT (1999)
- the Public Law and Public Administration discussion group, ANU (1999)

ASIO also makes a presentation to the annual Security in Government Conference. This conference, organised by the Protective Security Coordination Centre, was originally intended for government Agency Security Advisers. It has since been opened up to security advisers from private industry. ASIO's Protective Security section also has a stand at the conference, a fact which is usually reported in the media.

ASIO officers routinely address service clubs such as Rotary, Lions and Probus on request. Presentations have been made in regional centres as well as in the capital cities.

Each occasion an ASIO officer presents him or herself in such a circumstance, those attending usually have the opportunity to ask questions directly of the officer.

Letters from members of the public

ASIO receives approximately one letter a day from members of the public who are requesting or volunteering information. Many of the requests are from those seeking ASIO assistance and who have a mistaken belief about ASIO's role. In such cases, they are usually provided with an information leaflet about ASIO.

Others seeking information include school and university students who seek ASIO assistance with a project or assignment. In the case of the former, it is usually possible to help by providing information leaflets. For university students, the ASIO library provides assistance on the basis that our library is part of the inter-library loan system.

Administrative Appeals Tribunal

Two aspects of ASIO's activities are subject to appeal to the AAT.

Security Assessments

Part IV of the ASIO Act allows ASIO to provide security assessments to other Commonwealth agencies for people who require security clearances for access to classified information. Although the security clearance is granted by the employing agency, ASIO's assessment is used by agencies to assist them make that decision.

If ASIO provides an adverse or qualified assessment in respect of an individual, a copy of the assessment must be supplied to that person, unless the Attorney-General issues a

certificate stating that it would be prejudicial to the interests of security to provide the assessment, or part of the assessment, to the person concerned. The person may then appeal to the AAT against the assessment. The AAT may confirm or supersede the assessment.

There was one appeal during each of the last two reporting years. In both cases the ASIO assessment was upheld by the AAT.

In 1994 the PJC conducted an enquiry into the way in which ASIO performs its functions in relation to security assessments.

Requests under the Archives Act

ASIO has been subject to the Archives Act since its inception in 1983 in the same manner as other Commonwealth agencies. The public may request access to any documents which are more than 30 years old. Exemption of a whole document, or part of the text, can be claimed by ASIO on the basis of grounds stipulated in s33 of the Archives Act. ASIO limits exemptions to only that information which, if released, could reasonably be expected to damage Australia's national security. For practical purposes, most exemptions claimed by ASIO relate to protecting the identity of a confidential source of information.

The public can appeal against ASIO's decision to exempt information, initially by means of an Internal Reconsideration by the National Archives of Australia (NAA) and, if the applicant remains unsatisfied, they can appeal to the Security Division of the Administrative Appeals Tribunal. There has been a total of 29 appeals since 1986. The AAT made minor variations to ASIO's decision in six of these cases. In the remainder the appeal was either withdrawn, the ASIO decision affirmed or an agreement reached between ASIO and the appellant.

While ASIO's actions in relation to the Archives Act do not strictly fit within the definition of public reporting, these activities remain one of the most significant ways in which members of the public receive information about ASIO's past activities.

There is provision under the Archives Act for special access to material which is less than 30 years old. This access is only granted to those with an established record of scholarship who can demonstrate that the early release of the information will be of significant benefit to the Commonwealth. Special access has been granted four times by Directors-General, twice to professional historians and once each to a documentary film maker and a distinguished Australian writing his memoirs.

Recruitment

ASIO first advertised for Intelligence Officers in 1977 and was the first of the Australian intelligence agencies to do so. While public advertising is now common practice for many intelligence agencies, the British only placed their first advertisement in 1999 and the Canadian service still does not advertise publicly.

The overwhelming majority of ASIO vacancies are now advertised publicly, whether in the areas of intelligence collection, information technology, engineering, personnel, staff development or finance.

For a limited time in April/May 2000, ASIO appeared on the web site of an employment agency which was handling the advertising and initial selection for certain ASIO vacancies. The information related specifically to the positions being advertised. The recently launched ASIO web site includes job vacancies.

What ASIO does not report on

There are several aspects of ASIO's activities which are not reported publicly, including:

- ASIO's targets
- warrant operations (including operational methods)
- details of liaison with overseas agencies

ASIO's targets

ASIO does not publicly identify which groups, individuals, or foreign powers are ASIO 'targets' or subjects of investigation. This is because it would be extremely difficult, if not impossible, for ASIO to operate effectively if the subjects of investigation became aware of ASIO's interest in them. All target groups which ASIO investigates operate with varying degrees of secrecy. Many of the individuals concerned in activities which are prejudicial to national security go to extreme lengths to evade detection. If targets became aware of ASIO's interest in them, they would immediately take steps to alter their operations so as to diminish the likelihood of ASIO being able to mount a successful investigation.

ASIO is a relatively small organisation, in terms of its budget and the number of people it employs. This information is publicly known. Given its relatively small size, creating uncertainty among its targets is an important part of ASIO's modus operandi. If individuals, groups, or countries of security interest do not know whether ASIO is actively investigating them, they are forced to work harder than they otherwise might to avoid ASIO observation.

Public identification of ASIO targeting would highlight which groups, individuals or foreign powers were not the subject of ASIO investigation, which would indicate to them that ASIO was not aware of their activities.

Warrant operations

While ASIO's use of warrant operations (telecommunications and mail intercept, listening devices, entry and search, computer access and tracking devices) is publicly known, ASIO does not provide any public detail about the number of warrants executed each year, either by category, or in total.

Information about the number of different types of warrants ASIO has in place could allow an individual, group or foreign power to take counter-measures to avoid or reduce ASIO's ability to monitor their activities. For example, a breakdown of warrant numbers by type could reveal that ASIO relies most heavily on some types of special powers, while making more limited use of others. Target personalities or groups could use this information to avoid using the means of communication that they know ASIO is actively monitoring, which would deprive ASIO of information relevant to security.

Aggregated reporting of the total number of warrants, even if not broken down by type, would allow targets, including counter-terrorist targets and hostile intelligence services, to assess the level of risk to their activities, particularly when put together with other information in the public domain, such as ASIO's size, staff numbers, budget and legal regime.

For example, a smaller than expected number of warrants might lead targets to assess the level of ASIO coverage as low, and so their own activities against Australia could be increased. A higher than expected number of warrants might lead targets to assess the level of ASIO coverage as high, and cause them to find new ways of conducting activities against Australian interests.

If information on warrant types and numbers was considered along with information on ASIO's investigative and targeting priorities, a target's ability to make accurate assessments of the risk which ASIO posed to their operations would be even greater.

There are also difficulties associated with reporting both security intelligence and foreign intelligence warrant numbers. In addition to collecting security intelligence relevant to national security, ASIO collects foreign intelligence, under warrant, at the request of either the Minister for Foreign Affairs or the Minister for Defence. If ASIO specified publicly the total number of warrants issued this could lead to a misunderstanding in the community about the extent of ASIO's activities as they affect Australian citizens. Conversely, splitting the figure to show security and foreign intelligence warrants separately would be unacceptable to those Australian agencies which receive the foreign

intelligence product as it could indicate to their target groups how active they are in a particular intelligence collection area.

There is a considerable number of safeguards in place regarding how ASIO may collect intelligence. All operational activity by ASIO must be consistent with the Attorney-General's guidelines for the Collection of Intelligence which require ASIO to use methods of investigation which are consistent with the level of threat. Warrants are only submitted to the Attorney for approval after they been through an exhaustive system of checks within ASIO. Before consideration by the Attorney, the warrants and accompanying requests are examined by a senior official of the Attorney-General's Department, who provides independent advice to the Attorney on whether the relevant statutory requirements have been met. The Inspector-General also regularly reviews the warrant documentation.

Liaison with overseas agencies

ASIO is permitted under its legislation to liaise with "…the authorities of other countries…". Liaison with individual agencies requires the approval of the Attorney-General under section 19 of the ASIO Act.

ASIO's liaison relationships provide valuable and at times unique insights into matters of direct security relevance to Australia. All ASIO's relationships with foreign agencies are established on the basis of confidentiality. While the general principal of international liaison, and the number of countries and agencies with which ASIO has relationships is acknowledged publicly, the specific countries and services are generally not, unless both ASIO and the specific foreign agency agree to acknowledge the relationship publicly.

Foreign liaison, by its very nature, is bilateral and can only be undertaken in terms and conditions which are acceptable to both parties. If ASIO acknowledged a liaison relationship against the wishes of a cooperating agency, not only would that agency be reluctant to continue to exchange information with ASIO, but the breach would also be noted by others.

Comparisons with other Australian agencies

A brief review of the public reporting of sensitive matters by Australian agencies is provided at Appendix B.

Australian Intelligence Community

ASIO is the only member of the Australian Intelligence Community (ASIS, DSD, ONA, DIO[1]) to provide a public report to Parliament, although these organisations all provide classified reports to Ministers. This is consistent with ASIO's role as the intelligence agency which has the highest profile in the community and whose activities affect Australian citizens more so than other members of the intelligence community.

Law Enforcement Agencies

In comparison to ASIO, the state police services report similar information on corporate governance, management and accountability arrangements. The police services also report quite extensively on activities that rely on community support for their success, and they report the results of major operations in general terms, for example, the numbers of people arrested, or assets seized. This would seem to reflect the fairly public nature of police work, where successful operations result in publicly reported criminal prosecutions. A successful investigation will lead to a court appearance at which many of the methods used in the investigation will be described by witnesses when giving evidence. In contrast, ASIO's operational successes rarely result in prosecutions, but instead result in action which does not have a high profile, eg denial of a visa to enter Australia.

While the annual report of the Australian Federal Police (AFP), like ASIO's report, identifies a range of useful investigative methods including physical and electronic surveillance and telecommunications interception, the state police services do not make reference to covert operational capabilities or methods. Neither ASIO, the AFP or the state police services report the number or type of warrants sought or executed. The National Crime Authority does provide an overall figure for the number of telecommunications interception warrants issued during the year, together with comparative information from previous years.

Oversight Bodies

The annual reports of the NSW Independent Commission Against Corruption, the NSW Police Integrity Commission and the QLD Criminal Justice Commission do report details such as the number of telecommunications interception and listening device warrants obtained, and report in some detail on operational objectives and investigative outcomes. This may reflect the fact that the oversight bodies have a clear and publicly acknowledged target of investigation.

---

[1] ASIS – Australian Secret Intelligence Service, DSD – Defence Signals Directorate, ONA – Office of National Assessments, DIO – Defence Intelligence Organisation

In contrast, ASIO relies on creating uncertainty among its targets as an important part of its modus operandi (see page 16). And ASIO targets can be considerably better resourced than the targets of oversight bodies eg hostile intelligence services.

International comparisons

A comparison of the public reporting of the security services in those countries which have comparable standards of parliamentary democracy and human rights as Australia reveals a wide range in reporting practices. Appendix C provides this comparative information in chart format.

United Kingdom Security Service

The United Kingdom Security Service (UKSS, also referred to as MI5) does not produce a publicly available annual report, although it does produce a booklet describing its role and functions. Certain aspects of the UKSS's activities, including details of their resource allocation, are reported in the publicly available Intelligence and Security Committee's annual report.

The UKSS has, like ASIO, both a parliamentary committee and a Security Service Commissioner, the latter having a role similar to that of the IGIS. Like ASIO, the UKSS provides a general assessment of the security environment, and like ASIO, does not publicly identify its targets, its operational capabilities, or the number of warrant-type operations.

Federal Bureau of Investigation

The FBI does not produce an annual report; however, it has a web site which includes contact and employment information, and details of major initiatives and programs. Testimonies to Congress also have a high profile and usually provide focused information on specific topics. The FBI also has a large range of hardcover information booklets available to the public. Two examples of their publications are provided to the committee and listed at Appendix D.

In contrast to the other Australian and foreign services, the US government does provide some information regarding its intelligence targeting. This is not done directly by the FBI but via two other channels. The first is a compilation by the US State Department of the "National Register of the Designation of Foreign Terrorist Organisations" which lists those foreign terrorist organisations whose activities pose a threat to US interests. Although there is no requirement for the FBI to investigate those organisations, commonsense would suggest that is the case. At the very least, the publication of this list indicates to terrorist organisations that the full weight of US resources may be directed against them.

The second channel by which targets are identified is via evidence tendered in court for investigations which result in a trial. This clearly identifies not just the individuals but also organisations in which the FBI has an interest. However, the FBI takes steps to limit the amount of intelligence material, particularly regarding operational methods, which is provided in court. One way the FBI achieves this is by having two separate but parallel investigations, one criminal and one intelligence, with no sharing of personnel or paperwork. This separation results from the FBI's position as both an intelligence and police agency.

Canadian Security Intelligence Service

The Canadian Security Intelligence Service (CSIS) does produce an annual report but it is exceedingly summary in nature, being only 15-20 pages in length. It does not include any details of operational capabilities, warrant-type operations, or CSIS targets. CSIS also has a range of publicly available information, both on their web site and in hard cover. Examples of their publications are provided to the committee and are listed at Appendix D.

New Zealand Security Intelligence Service

The New Zealand Security Intelligence Service (NZSIS) currently produces a classified report for the Prime Minister and the parliamentary Intelligence and Security Committee. Starting in 2000-01, the NZSIS will also produce an unclassified version of this report for the Parliament, which is expected to include warrant-type statistics. The NZSIS also produces a booklet which provides a broad outline of the role and functions of the NZSIS.

Bundesamt für Verfassungsschutz

The Bundesamt für Verfassungsschutz (BfV) is Germany's domestic security service whose functions and responsibilities most closely mirror those of ASIO. The BfV uses its 160 page annual report as a major public reporting mechanism on the security environment. The report lists all of the groups which are of security interest, and provides detail on membership, leadership, publications and addresses of premises for each group. The report also specifies which countries are involved in the proliferation of weapons of mass destruction, and identifies those countries whose intelligence services pose a threat to Germany, together with details of their presence in Germany. It does not provide any information on intelligence collection capabilities, warrant-type operations, operational activities or liaison with other agencies. For the reporting of administrative type matters, there is a statement specifying the overall budget and number of employees. No other administrative detail such as structure is provided.

The German BfV is the only service surveyed which publishes such a detailed account of the security environment.

Direction de la Surveillance du Territoire

The Direction de la Surveillance du Territoire (DST) is the French security service. There is no public reporting or oversight of the activities of the DST. This includes an absence of a web site, annual report, publicity material and information concerning targeting, operational capabilities or the security environment. A review of France's intelligence services is presently underway.

Servizio per le Informazioni e la Securezza Democratica

The Servizio per le Informazioni e la Securezza Democratica (SISDE) is Italy's security service. It produces an unclassified annual report which is limited in its scope. Like most of the other security and intelligence agencies it does not include any details of operational capabilities, warrant-type operations or targets, but neither does it report on its structure, staffing or budgeting arrangements.

ASIO's future reporting plans

Discussion papers

ASIO has considered the benefits of publishing unclassified discussion papers on subjects of security interest, along the lines of discussion papers produced by the British and Canadian services. These papers would not contain any information about ASIO targeting or operational methods; rather they would provide overviews of issues of security significance, drawing on open source information.

Publication of such papers on the ASIO Web site could assist in the demystification of ASIO. However, at present ASIO does not have the resources to undertake this activity.

The web site

ASIO's web site provides new opportunities for ASIO to communicate with the public. As we gain experience with, and receive feedback on this means of communication, ASIO will consider other types of information that could usefully be made available on the web site, consistent with the constraints of security and resources.

Conclusion

ASIO endeavours to provide the public with as much information as possible, within the constraints of security and resources. The most visible aspect of ASIO's public reporting is the unclassified Report to Parliament. The public is also informed about ASIO's activities through the Annual Report of the Inspector-General, reports of the Parliamentary Joint Committee, and appearances before other parliamentary committees and the Administrative Appeals Tribunal. These activities are complemented by a range of other initiatives including occasional media interviews of the Director-General of Security, presentations to service clubs, conferences and other groups, the availability of a number of information publications, the release of information under the Archives Act, and public interaction with ASIO's Media Liaison Officer.

The launching of ASIO's web site will provide many more Australian citizens with easy access to information about ASIO. In terms of what information can be made publicly available, ASIO will always be more constrained than agencies that do not have a security intelligence function. As a security service, it is a reality that information that would be of most interest to the public (for example, details of targeting and operational capabilities, particularly those conducted under warrant) is exactly that information which would cause great harm to Australia's national security if it was publicly released.

This dilemma is faced by other security and intelligence services in Australia and overseas. In an international context, ASIO provides more information about its activities than most comparable agencies. Within Australia, ASIO is the only intelligence agency to provide a publicly available Report to Parliament,.

ASIO's current reporting activities achieve an appropriate balance between the need to protect its capability to advise government of threats to national security, with the need to properly inform the public of its activities.

Appendices

A. Significant dates in ASIO's public reporting history

B. Australian agencies – comparison with ASIO

C. Overseas services - comparison with ASIO

D. Attachments – publications provided to the PJC

Appendix A

Significant dates in ASIO's public reporting history

1949	ASIO established
1956	ASIO Act
1960	Telephonic Interception Act Amendments To Crimes Act re espionage and breaches of official secrecy
1977	Royal Commission into Intelligence and Security First public advertisements by ASIO for staff First public address by ASIO's Director-General (National Press Club)
1979	Amendments to ASIO Act Establishment of Security Appeals Tribunal
1983	First ASIO Report to Parliament Archives Act
1984	Royal Commission into Australia's Security and Intelligence Agencies
1985	Position of Media Liaison Officer established First media interview of ASIO's Director-General
1986	Amendments to ASIO Act Establishment of Parliamentary Joint Committee Establishment of Inspector-General of Intelligence and Security
1988	Attorney-General's Guidelines for Politically Motivated Violence tabled
1989	Attorney-General's Guidelines for Staffing tabled
1992	Attorney-General's Guidelines for the Collection of Intelligence tabled
1993	First ASIO unclassified Corporate Plan publicly available First ASIO appearance before Senate Estimates
1994	'Testing Security Products' - an information leaflet on protective security
1995	'What's ASIO about?' – an information leaflet 'What's the SCEC' - an information leaflet on protective security
1996	'ASIO now' - a booklet on ASIO
1998	'What's ASIO's role in protective security?' - an information leaflet
2000	ASIO web site launched on 22 June 2000

Appendix B

Australian agencies - comparison with ASIO

NSW Police Service

Like ASIO's report, the Annual Report of the NSW Police Service contains considerable detail about corporate governance and corporate reform. The report also includes information about crime rate trends, public satisfaction surveys and community liaison initiatives. The results of major operations are reported in general terms, for example, the numbers of people arrested and assets seized for each major operation. Unlike ASIO, the report makes no mention of the operational methods or capabilities (for example, telephone intercept or listening devices) available to the NSW Police.

Victoria Police

The Annual Report of the Victoria Police is similar in content to that of the NSW Police Service. High profile activities that rely on community support are reported on, as are corporate management issues. Reference is made to the increased demand for specialist technical investigative skills as a result of criminal use of the Internet, and to forensic procedures used to support investigations, but the report makes no mention of the operational methods or capabilities available to the Victoria Police.

Australian Federal Police

As the AFP has both community policing and national criminal intelligence responsibilities, its Annual Report has elements in common with those of the state police forces, as well as with ASIO's Report to Parliament. The AFP report provides an overview of the Commonwealth law enforcement environment, and like the NSW and Victoria Police reports, highlights operations that resulted in arrests or seizures of assets, and reports on community liaison initiatives. Like ASIO, the AFP identifies a range of useful investigative methods, including physical and electronic surveillance, telecommunications interception and extensive access to financial intelligence provided by the Australian Transaction Reports and Analysis Centre (AUSTRAC); however, like ASIO, the AFP makes no reference to details such as the number of warrants sought or executed.

Western Australia Police Service

The Annual Report of the WA Police Service provides similar information to that of the NSW and Victoria Police. Although it makes reference to the use of AUSTRAC

information (although statistical information is not provided), there is no reference to other investigative capabilities such as telephone interception.

South Australia Police

Similarly, the Annual Report of the South Australia Police does not refer to covert operational methods or capabilities.

Queensland Police Service

The Queensland Police Service refers to the use of telephone interception as an investigative tool, but like the other police and intelligence services, Queensland Police do not provide details of covert operational methods or capabilities.

National Crime Authority

The NCA Annual Report includes examples of positive operational outcomes, with some limited discussion of operational methods (for example, the benefits of public hearings, examination of financial transactions, etc). The report also provides an overall figure for the number of telecommunications interception warrants issued during the year together with comparative figures for the previous three years. Its 1998/99 report attributes a 50% increase in warrants since the previous year to increased funding for the National Illicit Drugs Strategy and the changing telecommunications environment.

Police Integrity Commission (NSW)

The Police Integrity Commission of NSW provides relatively specific reports of operational objectives in its Annual Report, and reports the number of warrants issued for telecommunications interceptions. The Commission also reports the number of search warrants and listening device warrants sought and executed during the reporting year, and comparative information from the previous two years. The Commission also holds public hearings, as a principle means of deterring police officers from engaging in various forms of serious misconduct, by demonstrating the extent of its reach and its capacity to obtain information and evidence by means of a variety of investigative methodologies.

Independent Commission against Corruption (NSW)

ICAC provides figures on the number of investigations conducted using listening devices, telephone interception, controlled operations and assumed identities during the reporting year, and comparative information from the previous year. Details of investigations for

which there have been public hearings are also provided in the annual report, although the report does mention that members of the public will generally not be aware of investigations for which there has been no public hearing or report. Although it is ICAC policy not to disclose operational details about matters which are not in the public domain, it does provide brief examples of a few subjects of investigation or preliminary inquiry.

Criminal Justice Commission (Qld)

Queensland's Criminal Justice Commission's (CJC) Annual Report includes case studies and examples of investigations undertaken, including the objectives of the investigation and the outcomes achieved. Some case studies include limited discussion of operational and investigation techniques employed. The CJC also reports the numbers of search warrants obtained and listening devices approved.

Overseas services - comparison with ASIO

The following table provides:

- a comparison of the principal methods by which overseas agencies report to the public
- the types of information made available

	ASIO	NZ (NZSIS)	UK (UKSS)	US (FBI)	Canada (CSIS)	Germany (BvF)	France (DST)	Italy (SISDE)
Reporting methods								
public annual report	Y	N[2]	N	N	Y	Y	N	Y
web site	Y	N	Y	Y	Y	Y	N	Y
leaflets/booklets	Y	Y	Y	Y	Y	N	N	N
Parliamentary[3]	Y	Y	Y	Y	Y	Y	N	Y
oversight bodies[4]	Y	Y	Y	Y	Y	Y	N	N

[2] First annual report expected for the year 2000-01

[3] This includes the equivalent of Australia's Parliamentary committees, Question Time, Questions on Notice

[4] Accountability mechanisms which are available to the public eg Inspector-General of Intelligence & Security

Appendix C

	ASIO	NZ (NZSIS)	UK (UKSS)	US (FBI)	Canada (CSIS)	Germany (BvF)	France (DST)	Italy (SISDE)
Types of information								
targeting	N	N	N	some	N	N	N	N
security environment	general description	general description	general description	general description	general description	detailed description	N	general description
foreign liaison partners	N	N	N	N	N	N	N	N
warrant-type statistics[5]	N	N[6]	N	N	N	N	N	N
operational capabilities	N	N	N	N	N	N	N	N
structure	Y	Y	Y	Y	Y	N	N	N
budget	Y	Y	Y	Y	Y	Y	N	N

[5] These comprise the operations for which ASIO would require a warrant from the Attorney-General – telecommunications and mail intercept, entry and search, listening devices and computer access.

[6] We understand the NZSIS will report warrant statistics for the year 2000-01.

Appendix D

Attachments - publications provided to the PJC

ASIO Reports to Parliament

Report to Parliament 1998-99

Report to Parliament 1982-83

ASIO publications

Corporate Plan 1998-2002

ASIO Now

What's ASIO about?

What's ASIO's role in protective security?

What's the SCEC?

Testing Security Products – the work of ASIO's security equipment testing site

Other Australian Agency reports

IGIS Annual Report 1998-99

Overseas Agency reports

MI5 – The Security Service (booklet)

NZSIS – Security in New Zealand Today (booklet)

FBI

- Fiscal Year 1998 Report – Office of Professional Responsibility
- Ensuring Public Safety and National Security under the Rule of Law

Canadian Security Intelligence Service (CSIS) – an information pack containing

- The 16 page Public Report.
- 'CSIS - in a Changing World'
- Awareness Brief – 'Economic Espionage', 'Computer Security'

Appendix D

- Backgrounder Series - ‘A Historical Perspective on CSIS’, ‘Accountability and Review’, ‘Economic Security’, ‘Counter-Terrorism’
- Perspectives - ‘Trends in Terrorism’
- Commentary - ‘LTTE International Organization and Operations – A Preliminary Analysis’ (written by an academic and expressing personal opinions)
- recruiting leaflet - ‘Intelligence Officer’
- information leaflet - ‘Welcome to Communications Branch’

Australian Security Intelligence Organisation

Supplementary Submission to the Parliamentary Joint Committee on ASIO

–

Access to ASIO's archival records

"An inquiry into the nature, scope and appropriateness of the way in which ASIO reports to the Australian public on its activities"

2 August 2000

Submission by ASIO

This submission was prepared in response to questions raised about access to ASIO's archival records during the Committee's public hearing on 17 July 2000. It supplements information about ASIO's public reporting provided in a submission dated 5 July 2000.

Attached to this submission is a report on ASIO's progress in addressing recommendations made by Parliamentary Joint Committee following its April 1992 inquiry into the effect on ASIO of the operations of the access provisions of the Archives Act.

ASIO and the Archives Act

No Commonwealth department or agency, including ASIO, is excluded from the operation of the *Archives Act 1983*. Members of the public may apply for access to any ASIO records more than 30 years old.

ASIO, like the other Australian intelligence agencies, has elected to retain custody of its archival records. This is provided for in s.29 of the Archives Act. ASIO also takes responsibility for assessing its archival records for public release and providing advice on exemptions to National Archives of Australia.

There are no ASIO specific provisions in the *Archives Act 1983*.

Public access to ASIO's archival records

Members of the public seeking access to ASIO archival records can only do so through National Archives. Between 1,500 and 2,100 ASIO items are issued through the National Archives' reading room each year. Around 10% of applications are for records that are not already in National Archives' custody. In these cases, National Archives forwards applications for access to ASIO.

On receipt of a new application, members of ASIO's Public Research section check its subject or subjects against ASIO's name and file indexes. If relevant records exist and are in the 'open access period' (more than 30 years old), they are collated, assessed and forwarded to National Archives, who make them available to the applicant and anyone else seeking access to them. National Archives makes the final access decision in all cases.

ASIO received 157 new applications due for completion in FY 1999/00, covering 264 separate items or subjects. Seventy-three percent were completed within 90 days (the time period allowed for in the Archives Act).

The following table shows ASIO's performance over the last seven reporting periods.

FY	No. of new applications (items)	90 day completion rate	No. of staff working on archives matters.
93/94	241 (1633)	82.5%	12
94/95	221 (644)	85.0%	11.5
95/96	270 (1121)	89.6%	10.5
96/97	214 (731)	65%	5 to 7.4
97/98	166 (375)	86%	8.4
98/99	186 (328)	75%	8.4
99/00	157 (264)	73%	8.4[1]

National Archives figures show that ASIO receives the third highest number of applications for access to archival records, behind the Department of Foreign Affairs and Trade (DFAT) and the Department of Defence. ASIO devotes a much higher percentage of its resources to archives work than either of those departments, or any other Australian intelligence agency.

The following table compares ASIO's workload and resource allocations to those of DFAT, the agency that receives the highest number of applications.

	DFAT	ASIO
Staff in agency in FY 1998/99	3,633	513
Number of Archives Act applications in FY 1998/99	521 applications (213 public; 258 official; 50 special access)	186 applications (for 328 subjects)
Staff working on examining files for release under the Archives Act	5.5 (0.15% of total staff)	8.4 (1.64% of total staff)

[1] ASIO staff working on Archives Act applications are being re-deployed to meet Sydney 2000 Olympic Games security intelligence priorities. Time spent to date on Olympics-related training and preparation accounts for much of the decline in the 90-day response rate in FY 99/00.

ASIO archival records require more extensive assessment for public release than those of other agencies. Many file series in other agencies contain little or no sensitive information and can be released without document-by-document, line-by-line examination. All ASIO files, however, contain classified or otherwise sensitive information.

ASIO officers must examine each document to determine whether release could affect confidential sources, liaison relationships, and methods of collecting intelligence. They must be aware that release of information can aid in building a comprehensive picture through a process we describe as 'mosaic analysis'. This is a method by which a persistent researcher can, for example, identify a confidential source by bringing together seemingly unconnected pieces of information on different documents and files.

Who seeks access to ASIO's archival records?

National Archives does not, as a matter of policy, provide ASIO with the names of individuals making applications for its archival records. National Archives withholds names on information privacy grounds.

National Archives does, however, invite applicants to indicate that they are seeking access to their own records, or those of close family members ('family requests'). If they do, the Archives includes the information with the application passed to ASIO. 'Family requests' are given priority and most are completed within 90 days. Many are from individuals who were members of the Communist Party of Australia in the 1950s and 1960s.

'Family requests' made up 36% of the new applications due for completion in FY 1990-00. Ninety percent of these were finalised within 90 days. A total of 2,820 folios or pages were assessed in response to these completed 'family requests'. Fourteen percent of the folios were released without exemption; 64% were partially released; and 22% were claimed as wholly exempt and not transferred to the Archives.

Some major researchers also choose to make themselves known to ASIO. Their requests typically absorb around 25% of the resources ASIO devotes to archives work.

What do they receive?

If members of the public lodge an application for ASIO archival records with National Archives – and the records they are seeking exist - they can expect to receive something in response. It is also true that virtually all files released to National Archives by ASIO contain some exemptions.

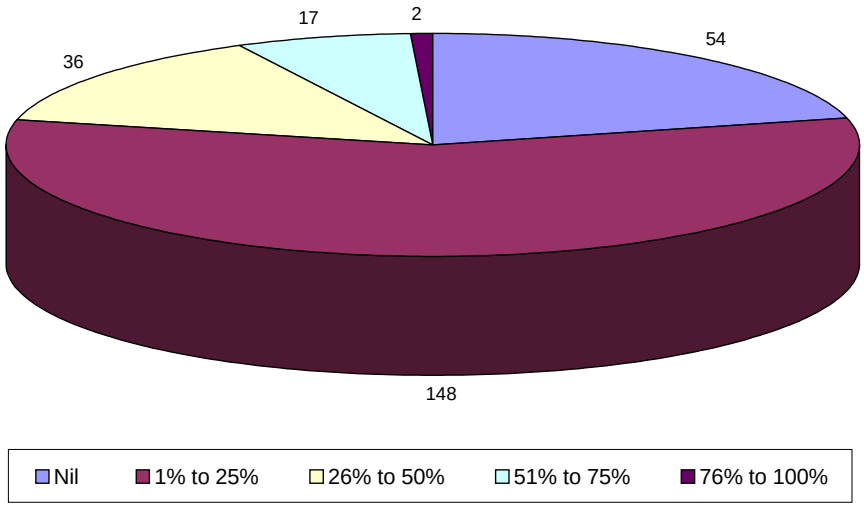
ASIO has not placed any class of its records outside the public access provisions of the Archives Act. We do, however, claim the personnel and security records of ASIO officers as wholly exempt on the basis of s.92(1) of the ASIO Act[2].

A proportion of the applications ASIO receives each year are for subjects that are either 'no trace' in our indexes, or for which there are no records in the open access period. ASIO gave a 'no trace' response to 22% of applications we received in FY 1999/00.

ASIO assessed more than 27,000 folios (pages) for public release in FY 1999-00. 21% were released without ASIO claiming exemption for any of the information they contained. Sixty percent were partially released. Nineteen percent were claimed as totally exempt because their disclosure could reasonably be expected to reveal the identity of a confidential source. These folios are not transferred to National Archives.

Two hundred and fifty-seven files containing wholly released and partially exempt folios were transferred to National Archives in FY 1999/00. Each file contained as few as one, or as many as 340 folios, depending on the number of records in the open access period. The following diagram and table show the distribution of totally exempt folios across those 257 files.

No. of Files released in 1999-2000 by the percentage of totally exempt folios they contain



[2] Section 92(1) of the *Australian Security Intelligence Organisation Act 1979* makes it an offence to make public that a person having a particular name is an officer or former officer of ASIO.

Files released to National Archives in FY 1999-2000	No. of files (folios)	% of total files (folios)
Category 1 – No totally exempt folios	54 (975)	*21% (4%)*
Category 2 - 1% to 25% totally exempt	148 (19,026)	*58% (70%)*
Category 3 - 26% to 50% totally exempt	36 (5,013)	*14% (19%)*
Category 4 - 51% to 75% totally exempt	17 (2,039)	*7% (8%)*
Category 5 - 76% to 100% totally exempt	2 (8)	*1% (0%)*

ASIO only claims exemptions where disclosure of the information could reasonably be expected to:

- Damage the security, defence or international relations of the Commonwealth [s.33(1)(a) of the Archives Act]; and/or

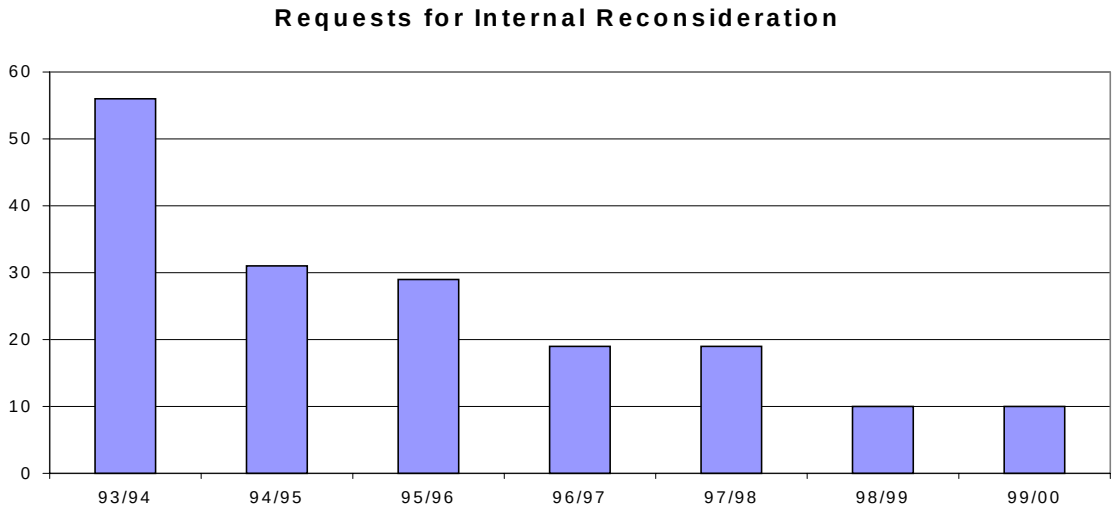
- Disclose or enable a person to ascertain the existence or identity of a confidential source [s.33(1)(e)(ii) of the Archives Act].

National Archives is responsible for claiming other exemptions in ASIO records [e.g. on personal privacy grounds, s.33(1)(g) of the Act].

Review of exemption decisions.

Applicants who are dissatisfied with the exemption claims can request an internal reconsideration under s.42 of the Archives Act. ASIO and National Archives officers jointly conduct internal reconsiderations. Because of the care put into the original decisions, most now result in minor or no change to the original decision.

The following graph shows the number of internal reconsideration applications received by ASIO in the last seven reporting periods.



The downward trend correlates with changes in ASIO's policy, designed to ensure that everything that can be released, is released at the initial assessment.

Further releases at the reconsideration stage are generally the result of approvals from ASIO's domestic and foreign liaison partners to release material provided by them. ASIO does not consult them at the initial stage, as the process is typically very slow and would delay researchers' access to other records.

Applicants dissatisfied with internal reconsiderations may then appeal to the Security Appeals Division of the Administrative Appeals Tribunal (AAT). The Tribunal may affirm the original decision to exempt or grant access to a record.

To date, there have been 30 AAT appeals concerning ASIO archival records, the first in February 1986. The following table shows their outcomes.

Exemption decision affirmed by the AAT	**6**
Exemption decision affirmed by AAT, with minor variations	**7**
Consent decision – mutually settled	**6**
Withdrawn by applicant	**11**
Exemption decision overturned by AAT	**Nil**

The cases that were resolved through negotiations between the parties ('consent decisions – mutually settled') resulted in either the release to the applicant of material previous claimed as exempt, or an explanation of the nature of the exempt material and the reasons for exemption sufficient to ameliorate the applicant's concerns.

Progress against PJC recommendations

"ASIO and the Archives Act: the effect on ASIO of the operation of the access provisions of the Archives Act" - April 1992

Recommendation 1: That guidelines be issued by the Minister to the Intelligence Agencies requiring that foreign material received in confidence should be exempted from disclosure for such period as that material is restricted from public access in the country of origin.

In practice, all information provided by foreign government agencies is claimed to be exempt unless the originating agency agrees to its release. The information is exempt because it could reasonably be expected to reveal the identity of a confidential source of information, and damage the security, defence or international relations of the Commonwealth. The AAT has consistently upheld our claim to exempt foreign-sourced information.

Recommendation 2. That the Archives Act should be amended to preclude any appeal to the Administrative Appeals Tribunal from a certification by the Inspector General of Intelligence and Security that the guidelines issued by the Minister respecting protection of foreign derived material has been properly observed.

Not actioned, legislative amendment required.

Recommendation 3. That the suppression of the identity of operatives, agents and sources, should be guaranteed in guidelines for a period of 30 years from the death of the operative, agent, or source.

In practice, all information that could reasonably be expected to disclose or enable a person to ascertain the identity of a confidential source of information is claimed as exempt from public release. The AAT has consistently upheld our claims to exempt such information.

Recommendation 4. That there should be no provision made to enable ASIO to exclude records from public access on the grounds of privacy unrelated to security.

ASIO only claims exemptions that are relevant to national security. National Archives claim privacy exemptions affecting ASIO records.

Recommendation 5. That ASIO records continue to be subject to the access provisions of the Archives Act. The open access period in respect of ASIO records should continue to be 30 years from the creation of the record. ASIO should continue to be obliged to make records in the open access period available save where the record is an exempt record under section 33 of the Archives Act.

ASIO records continue to be subject to these provisions of the Archives Act.

Recommendation 6. That Conclusive Certificates issued under the Archives Act should be subject to a 'sunset clause'. Section 34 of the Act should be amended to specify that a Conclusive Certificate issued by the Minister under the provision shall lapse after three years from the day it came into effect.

Not actioned, legislative amendment required. In its 1997 review of the Archives Act, the Australian Law Reform Commission (ALRC) recommended that Conclusive Certificates cease to have effect after 5 years, but be renewable. ASIO supported this recommendation.

Recommendation 7. That subsection 42(3) of the Archives Act relating to internal reconsideration of decisions should be amended to make it clear that the proper officer to make the decision on an application regarding access to records of ASIO should be the Director General of Security.

ASIO and National Archives staff jointly conduct Internal Reconsiderations and agree on a decision, although National Archives continues to be the formal respondent.

The ALRC recommended that this be altered so that the responsibility for reviewing a decision rests with the agency which has responsibility for making the initial decision - whether this is the National Archives or another responsible agency acting in accordance with an access agreement. ASIO supported this recommendation.

Recommendation 8. That an applicant for an internal reconsideration dissatisfied with the decision of the Director General of Security should be entitled to have that decision reviewed by the Inspector General of Intelligence and Security who should report his findings to the Minister who should determine the matter.

An applicant dissatisfied with the result of an Internal Reconsideration can appeal to the Administrative Appeals Tribunal (AAT). The AAT has affirmed, sometimes with minor amendments, ASIO/National Archives' decisions in all recent cases.

Recommendation 9. That there should be a right of appeal to the Administrative Appeals Tribunal from the decision of the Minister except in the circumstances referred to in Recommendation 8.

See the comment on Recommendation 8.

Recommendation 10. That the Government ensure that ASIO is provided with the necessary resources to enable it to discharge its statutory obligations under the Archives Act.

ASIO tripled resources in response to the 1992 PJC recommendations. In recent years, resources devoted to Archives issues have been reduced, as a result of further downsizing of the Organisation generally, but still remain well above 1992 levels. ASIO has a higher percentage of staff working on archives activities than any other agency of the Australian intelligence community. It also has a higher percentage of staff working on public access matters than either the Department of Defence or the Department of Foreign Affairs and Trade (DFAT).

Recommendation 11. That ASIO establish a special Archives Unit within the Organisation to manage applications for access to ASIO records in the open access period. The Unit should:

a. be headed by a senior intelligence officer qualified as an historian/archivist whose identity should be capable of being known to the public and who should be authorised by ASIO to negotiate with researchers on behalf of the agency;

b. develop indices and finding aids that can be made available to the public without infringing national security;

c. devote some resources to preparing records, in advance, for release as they fall into the open access period.

ASIO has established and maintained a Public Research section that responds to archives applications and manages all aspects of the Organisation's responsibilities under the Archives Act. A senior intelligence officer currently heads it. National Archives routinely provides researchers with the direct telephone number of ASIO's Director, Information Policy (D/IP) who has management responsibility for the Section. D/IP can negotiate on ASIO's behalf. Her name is made known to researchers once they have contacted ASIO.

Indexes and finding aids cannot be made available to the public without risking serious detriment to national security. ASIO's indexes and file registers provide very detailed evidence of the nature and scope of ASIO's activities. Whilst our activities are now broadly discussed in the unclassified Annual Report, the specific areas of intelligence interest, and the detail of ASIO's activities are not publicly known, and would cause damage to security if they become known.

ASIO realises that by not transferring our control records to National Archives, researchers will find it more difficult to access ASIO's records. We now actively seek to assist researchers in finding the records they want. Following the recommendations of the IGIS and the PJC in 1992, a policy of more open communication with researchers was adopted. ASIO officers will now help applicants refine and focus their applications, gain an understanding of their publishing schedules, and accommodate special requirements. However, ASIO's ability to do this is restricted by National Archives' policy of withholding the names of individuals making applications for ASIO records.

ASIO already commits a higher percentage of resources to archives-related activities than any other Australian intelligence agency, and, in fact, a higher percentage of resources than DFAT and Defence each commit to their public access responsibilities (Archives and Freedom of Information). We cannot afford to commit more resources to this function. Given the numbers of applications we receive each year, devoting resources to pro-active assessment of records would seriously damage our efforts to respond to new applications within 90 days and clear already back-logged applications.

Recommendation 12. That guidelines be developed under section 8A of the ASIO Act to facilitate spot checks by the Inspector General of Intelligence and Security and reviews of complaints as envisaged by the Committee in Recommendation 8.

ASIO now provides the Inspector General with detailed reports on our Archives activities.

Recommendation 13. That the proposed Archives Unit adopt a procedure that would categorise applications according to the following criteria:

a. fast track: where the application is small in resource terms, eg, individuals requesting their own files or that of a family member. These applications should be met within the 90-day statutory deadline;

b. bulk access: for those applications of a more complicated nature where access to material over a broad spectrum is desired. The researcher should be able to negotiate with ASIO both in regard to the scale of the application and the time in which it can be provided.

ASIO gives highest priority to applications from individuals seeking records relating to themselves or their immediate family. In most cases, these applications are completed within 90 days. However, we are aware that this approach could, if not managed carefully, see large applications from professional historians and other researchers 'slip to the bottom of the pile'. Consequently, during the last year, around 25% of the staff resources devoted to Archives work were used to meet this second category of application.

ASIO has adopted a policy of more open communication with researchers. We now seek to help them refine and focus their applications, gain an understanding of their publishing schedules, and accommodate special requirements. Our ability to do this is circumscribed by National Archives' policy of withholding the names of researchers making applications for ASIO records.

Recommendation 14. That in relation to current intelligence records, a person who wishes to ensure that information concerning himself/herself is accurate, may bring that information to the attention of the Inspector General of Intelligence and Security who will bring it to the attention of the responsible Intelligence Agency for appropriate action.

This facility now exists through the IGIS. ASIO has also negotiated an arrangement with National Archives whereby individuals who believe that ASIO archival records released to National Archives contain inaccurate or misleading information can apply to have a statement identifying and correcting these errors appended to the relevant file holdings.

SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE

Question No. 125

Senator Payne asked the following question at the hearing on 24 May 2005:

AUSTRAC's International role:

a) What liaison does AUSTRAC do with Australian agencies (such as the AFP) that are already represented in those Pacific or S-E Asian countries beforehand and during that process?

b) Could you identify for the committee where there are any gaps in the development of FIUs where you think there is more that could be done and where Australia can make a greater contribution as well?

The answers to the honourable senator's questions are as follows:

a) AUSTRAC is currently conducting three technical assistance and training programs: the South East Asia Counter Terrorism (SEACT) Program, Pacific Financial Intelligence Units Database Project (PFIUDP) and contribution to the Jakarta Law Enforcement Centre (JCLEC) initiative. During development of the three AUSTRAC technical assistance and training programs, AUSTRAC initiated meetings with senior officers from the Department of Foreign Affairs and Trade (DFAT), the Australian Agency for International Development (AusAID), Attorney-General's Department (AGD), Australian Federal Police (AFP) and other non-government agencies to establish relationships, ascertain donor activity within the South East Asian and Pacific regions and provide an overview of AUSTRAC initiatives within these regions. This liaison ensured AUSTRAC's programs had the support of relevant Australian agencies and were developed in a form that complemented existing work of Australian agencies in South East Asia and the Pacific.

Effective delivery of these technical assistance and training programs involves ongoing liaison with the above agency's representatives in Australia and at overseas posts. The ongoing liaison with Australian agency representatives overseas involves meetings and briefings with DFAT, AusAid and the AFP. AUSTRAC staff travel to the ten South East Asian (Brunei, Cambodia, Indonesia, Laos PDR, Malaysia, Myanmar, Singapore, Thailand, the Philippines and Vietnam) and seven Pacific (Cook Islands, Fiji, Marshall Islands, Palau, Samoa, Tonga and Vanuatu) jurisdictions that are being provided with assistance under these programs.

b) AUSTRAC is currently providing a range of assistance to counterpart organisations in the South East Asian and Pacific regions under the SEACT, PIFIUDP and JCLEC initiatives. AUSTRAC assistance is being provided in the form of in-country mentoring, IT advice, training programs, database development and hardware purchases, and assistance with typologies development.

In South East Asia the Governments of Indonesia, Malaysia, Singapore, Thailand and The Philippines have established fully operational FIUs. The Governments of Brunei, Cambodia, Laos, Myanmar and Vietnam are currently working towards establishing operational FIUs.

AUSTRAC's SEACT program is primarily focussed on delivering tailored assistance packages which recognise the differing needs of these two subsets of nations.

AUSTRAC is working with the FIUs in Indonesia, Malaysia, Singapore, Thailand and The Philippines to advance their skills, enhance their IT systems and promote effective interaction with other government agencies involved in anti-money laundering and counter-terrorism financing programs. In Brunei, Cambodia, Laos, Myanmar and Vietnam, AUSTRAC assistance is focussing on awareness raising and FIU design and implementation issues.

In the Pacific region the Governments of the Cook Islands, Fiji, Marshall Islands, Palau, Samoa, Tonga and Vanuatu have established small FIUs, while other Pacific Island nations are currently exploring FIU establishment.

AUSTRAC also works closely with other donors to collectively provide capacity building assistance in the detection of money laundering and terrorist financing activity. Where AUSTRAC identifies related needs which are outside its area of expertise, it raises these needs with other donors.

AUSTRAC also works closely with the Asia Pacific Group on Money Laundering (APG), as the APG is the regional body which coordinates technical assistance and training and assists with the adoption, implementation and enforcement of internationally accepted standards against money laundering and terrorist financing.

AUSTRAC is working with the Attorney-General's Department as it establishes the Financial Intelligence Support Team (FIST) Program. The FIST program will provide effective mentoring to Governments in the Pacific to aid development of strong anti-money laundering and counter-terrorism financing programs.

In addition, AUSTRAC is also exploring an option to work under AusAID's Pacific Governance Support Program (PGSP) to assist the Reserve Bank of Fiji with IT development for the Fiji FIU.