

ANTI-TERRORISM LAWS

A GUIDE FOR COMMUNITY LAWYERS



Federation of
Community Legal Centres
VICTORIA

Anti-Terrorism Laws Working Group

ANTI-TERRORISM LAWS

A GUIDE FOR COMMUNITY LAWYERS



Federation of
Community Legal Centres
VICTORIA

Anti-Terrorism Laws Working Group

This guide was prepared by Marika Dias and Patrick Emerton on behalf of the Anti-Terrorism Laws Working Group of the Federation of Community Legal Centres (Vic) Inc.

Copyright

© 2008 Federation of Community Legal Centres (Vic) Inc.

This guide is copyright. Community organisations and individuals may copy parts of this guide for not-for-profit purposes, as long as the original meaning is maintained and there is acknowledgement of the Federation of Community Legal Centres (Vic) Inc.

This guide can be downloaded from our website at: www.communitylaw.org.au

Disclaimer

The information in this guide is current at June 2008 but it may change without notice. The information in the guide is in the nature of general comment only and does not constitute, and should not be used as a substitute for, legal advice on any particular matter. Users of the guide should not act on any material or information in the guide without obtaining legal advice relevant to their own particular issue. The Federation of Community Legal Centres (Vic) Inc and the persons involved in researching, drafting and editing this guide expressly disclaim any liability to any person or entity in respect of any action taken or not taken in reliance on the guide's contents.

This publication has been supported with a grant from the Victoria Law Foundation – www.victorialaw.org.au



CONTENTS

Introduction..... 1

Definition of 'Terrorist Act' 2

Terrorism Offences..... 3

Definition of 'Terrorist Organisation' 6

Listing of Terrorist Organisations..... 7

Terrorist Organisation Offences..... 8

Financing Terrorism 13

ASIO and the AFP..... 15

ASIO's Powers..... 16

AFP Powers..... 47

Special Police Powers..... 52

Victoria Police..... 55

Control Orders..... 58

Preventative Detention 61

National Security Information Legislation..... 65

Sedition..... 67

More Information and Resources..... 69

INTRODUCTION

Since 11 September 2001, Australia's Federal and State governments have enacted new laws to deal with 'terrorist' activity. These laws do the following:

- Define a 'terrorist act' and a 'terrorist organisation'.
- Create new criminal offences relating to terrorist acts and terrorist organisations.
- Provide the government with the power to list organisations as terrorist organisations.
- Create criminal offences in relation to financing terrorism and financing terrorist organisations.
- Give further powers to the Australian Security Intelligence Organisation (ASIO) when it is gathering intelligence relating to terrorist acts.
- Give further powers to the Australian Federal Police (AFP) when they are investigating terrorism-related offences.
- Allow the AFP to obtain documents relating to serious terrorism offences.
- Give special powers to all police to stop, search and question people when authorised.
- Give power to Victoria Police to conduct covert searches.
- Provide for preventative detention and control orders.
- Prevent disclosure of information in federal criminal and civil proceedings where the disclosure is likely to prejudice national security.
- Provide for newly drawn sedition offences.

This Guide provides general information for lawyers on these aspects of Federal and Victorian State anti-terrorism legislation.



DEFINITION OF 'TERRORIST ACT'

Section 100.1, Part 5.3, Schedule 1, *Criminal Code Act 1995* (Cth) ('Criminal Code')

The *Criminal Code* provides a definition of what constitutes a 'terrorist act'. This is a broad definition on which most of Australia's other anti-terrorism legislation hinges.

A 'terrorist act' is defined as an action or a threat of action:

- that is done with the intention of advancing a political, religious or ideological cause;
AND
- that is done with the intention of coercing or influencing by intimidation a government of the Commonwealth, State, Territory, foreign country or the public or a section of the public; AND
- that causes or threatens to cause:
 - serious physical harm to people OR
 - serious property damage OR
 - a person's death OR
 - endangerment to people OR
 - a serious risk to public health or safety OR
 - serious interference with an electronic system.

It is important to remember that a 'terrorist act' does not have to be an actual action but can be simply a threat of such action.

Extended geographical jurisdiction applies to the definition of 'terrorist act'. This means that it may be something that occurs either in Australia or overseas.

Exceptions

Industrial action, advocacy, protest and dissent are all exceptions to this definition provided they are not intended to cause serious physical harm, death, endangerment or a serious risk to the health and safety of the public.



TERRORISM OFFENCES

Sections 101.1–101.6, Part 5.3, Criminal Code

It is an offence to commit a terrorist act (as defined above). The maximum penalty for this offence is life imprisonment.

In addition, stemming from the above definition of a 'terrorist act', are a range of terrorism offences. It is an offence to

- provide or receive training connected with preparation for, or engagement of a person in, or assistance in, a terrorist act (maximum penalty: 25 years knowingly or 15 years recklessly);
- possess a thing connected with a terrorist act (maximum penalty: 15 years knowingly, 10 years recklessly);
- collect or make documents likely to facilitate a terrorist act (maximum penalty: 15 years knowingly, 10 years recklessly);
- do any act in preparation for or planning for a terrorist act (maximum penalty: life imprisonment).

All of these offences can be committed knowingly or recklessly. The Criminal Code defines recklessness at section 5.4, division 5 as follows:

- A person is reckless with respect to a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
- A person is reckless with respect to a result if he or she is aware of substantial risk that the result will occur and having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

The question of whether a risk is 'substantial' depends on whether the 'reasonable observer' would have taken it to be substantial. It is, however, unclear exactly what would amount to 'substantial' in the eyes of a 'reasonable observer'. While some cases have adopted a 'more likely than not' test and refer to likelihood and probability, academic discussions appear to conclude that recklessness extends to 'possible risks', which include anything in excess of a 'bare logical possibility'. The question of whether taking a risk is unjustifiable is a question of fact. This means that it is a matter for a jury to determine. Once a person is aware of a 'substantial risk', however, it would seem that an acceptable justification for taking the risk would have to be something in the order of a sudden or extraordinary emergency. Anything short of an emergency would be unjustifiable.

...the offences encompass terrorist acts and offences that occur outside Australia.

(See: Ian Leader-Elliott, *The Commonwealth Criminal Code: A Guide for Practitioners*, Commonwealth Attorney-General's Department, March 2002)

Extended geographical jurisdiction applies to each of these terrorism offences. This means that the offences encompass terrorist acts and offences that occur outside Australia.

For the purposes of these offences, it does not matter whether the terrorist act has actually occurred or not. It also does not matter whether the terrorist act referred to is a specific act or not.

These offences have been broadly drafted. In particular, they are broad because they hinge on the definition of 'terrorist act', which itself is very broad and includes mere threats. Furthermore, each of the offences is broadly framed in itself. For example, the offence of giving or receiving training does not specify a definition for 'training'. This means that the 'training' in question could technically include training in first aid or business accounting, for example, as long as the relevant connection between the training and a terrorist act can be shown.

In the case of *R v Lhodi* [2006], trial judge Justice Whealy noted the pre-emptory nature of the offences and how the terrorist act involved will impact on sentencing:

[T]he legislation under which these offences has been created was specifically set up to intercept and prevent a terrorist act at a very early or preparatory stage, long before it would be likely to culminate in the destruction of property and the death of innocent people. The very purpose of the legislation is to interrupt the preparatory stages leading to the engagement in a terrorist act so as to frustrate its ultimate commission. An evaluation of the criminal culpability involved in any particular offence requires an analysis not only of the act itself, which may be relatively innocuous, but as well an examination of the nature of the terrorist act contemplated, particularly in the light of the intentions or state of mind of the person found to have committed the offence.

R v Lhodi [2006] NSWSC 691 [51]

The New South Wales Court of Appeal has also commented on the pre-emptory nature of the offences:

It was, in my opinion, the clear intention of Parliament to create offences where an offender has not decided precisely what he or she intends to do. A policy judgment has been made that the prevention of terrorism requires criminal responsibility to arise at an earlier stage than is usually the case for other kinds of criminal conduct, e.g. well before an agreement has been reached for a conspiracy charge. The courts must respect that legislative policy.

The legislation under which these offences has been created was specifically set up to intercept and prevent a terrorist act at a very early or preparatory stage...

Lodhi v R [2006] NSWCCA 121 [66], per Spigelman CJ

It is not necessary that the person accused of one of these offences have a terroristic intention, provided that s/he knows of, or is reckless in respect of, such an intention on the part of another:

[I]t is not, in my opinion, an essential element of the offence that an accused charged with doing any one of the acts identified in s101.4, s101.5 or s101.6 must himself or herself have the intention that the act advances a particular cause or is done with the requisite purpose of coercion or intimidation. Nevertheless, as an essential physical element, [such an intention and purpose] should be pleaded [by the Crown], but no particularity is required as to the person who had the relevant 'intention'.

Lodhi v R [2006] NSWCCA 121 [90], per Spigelman CJ



DEFINITION OF 'TERRORIST ORGANISATION'

Section 102.1, Part 5.3, Criminal Code

In the Criminal Code, a terrorist organisation is defined as an organisation:

- that is directly or indirectly engaged in preparing, planning, assisting in or fostering the doing of a terrorist act; OR
- that has been listed as a terrorist organisation by the government.



LISTING OF TERRORIST ORGANISATIONS

An organisation is eligible to be listed as a terrorist organisation by the government if the Attorney-General is satisfied on reasonable grounds that it:

- is directly or indirectly engaged in preparing, planning, assisting in or fostering the doing of a terrorist act; OR
- advocates the doing of a terrorist act, meaning that it:
 - directly or indirectly counsels or urges a terrorist act; OR
 - directly or indirectly provides instruction on doing a terrorist act; OR
 - directly praises the doing of a terrorist act where that praise may lead a person to engage in a terrorist act

Once again, the criteria for listing an organisation also hinge on the definition of 'terrorist act'.

The Director-General of ASIO has said that when recommending listing, ASIO takes the following into account:

- the organisation's engagement in terrorism;
- the ideology of the organisation and its links to other terrorist groups and networks;
- the organisation's links to Australia;
- the threat posed by the organisation to Australian interests (in Australia and overseas);
- the proscription of the organisation by the UN or by other like-minded countries; and
- whether or not the organisation is engaged in a peace or mediation process.

To date, the following organisations have been listed in Australia:

- | | |
|--|---|
| • Abu Sayyaf Group | • Islamic Movement of Uzbekistan |
| • Al Qa'ida | • Jaish-i-Mohammed |
| • Ansar al-Islam | • Jemaah Islamiyah |
| • Armed Islamic Group | • Kurdistan Workers Party (PKK) |
| • Asbat al-Ansar | • Lashkar I Jhangvi |
| • Egyptian Islamic Jihad | • Lashkar-e-Tayyiba |
| • Hamas's Izz al-Din al-Qassam Brigades | • Palestinian Islamic Jihad |
| • Harakat Ul-Mujahideen | • Salafist Group for Call and Combat |
| • Hizballah External Security Organisation | • Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn (the al-Zarqawi network) |
| • Islamic Army of Aden | |

TERRORIST ORGANISATION OFFENCES

Sections 102.2–102.8, Part 5.3, Criminal Code

The Criminal Code provides for a number of offences relating to terrorist organisations. These offences relate to both organisations that have been listed as terrorist organisations by the government and organisations that have not been listed but that fall within the first part of the definition of a terrorist organisation contained in section 102.1 (see page 2).

First, it is against the law to knowingly be a member of a terrorist organisation. To be classified as a member of a terrorist organisation you must either:

- formally or informally join the organisation OR
- take steps to join the organisation.

The maximum penalty for this offence is 10 years' imprisonment. Persons may have a defence to this charge if they can prove on the balance of probabilities that they took all reasonable steps to cease to be a member after they found out that it was a terrorist organisation.

...it is against the law to knowingly be a member of a terrorist organisation.

Other terrorist organisation offences are:

- Directing the activities of a terrorist organisation (maximum penalty: 25 years knowingly, 15 years recklessly).
- Intentionally recruiting someone to join or participate in the activities of a terrorist organisation (maximum penalty: 25 years knowingly, 15 years recklessly).
- Giving training to or receiving training from a terrorist organisation. The legislation does not indicate that there needs to be a link between the training and any terrorist activity. Since there is a separate offence of providing or receiving training in connection with a terrorist act (see page 3), it would seem that this offence may be triggered by any form of training. This was pointed out by Justice Hayne of the High Court in a case relating to a 'control order' against Jack Thomas (see section on Control Orders at page 58). This means that the training could be for innocent purposes such as first aid training, business accounting or fire safety (maximum penalty: 25 years knowingly or recklessly).
- Getting funds to, from or for a terrorist organisation. This offence may be committed where a person receives funds from or gives funds to a terrorist organisation (directly or indirectly) OR where a person collects funds for or on behalf of a terrorist organisation (directly or indirectly) (maximum penalty: 25 years knowingly, 15 years recklessly).
- Providing support or resources to a terrorist organisation where the support or resources would help the organisation directly or indirectly, engage in preparing, planning, assisting in or fostering the doing of a terrorist act (maximum penalty: 25 years knowingly, 15 years recklessly).

- Associating with a terrorist organisation. If a person:
 - intentionally meets on 2 or more occasions with another person who is a member of or who promotes or directs the activities of a listed terrorist organisation; AND
 - the first person knew that the organisation is a terrorist organisation; AND
 - the association provides support to the terrorist organisation; AND
 - the first person intends that the support will assist the organisation to expand or to continue to exist; AND
 - the first person knows about the second person's involvement in the terrorist organisation.

If a person has previously been convicted of this offence, any further association such as the above may attract the offence again, even if it does not occur on 2 or more occasions (maximum penalty: 3 years' imprisonment).

Exceptions to this offence are:

- where the association is with a close family member and relates to a matter of family or domestic concern;
- where the association is in a public place of religious worship and takes place in the course of practising a religion;
- where the association is only for the purpose of providing humanitarian aid; or
- where the association is only for the purpose of providing legal advice or legal representation in connection with certain types of legal matters. These include criminal proceedings and proceedings relating to whether the organisation is indeed a terrorist organisation, among other things.
- Note: The Attorney-General's Department has indicated that fundraising for the legal representation of those charged with terrorism offences would not attract the association offence.

For discussion of the concept of recklessness see above at page 3.

Extended geographical jurisdiction applies to each of these terrorism offences. This means that the offences can encompass activity that occurs outside Australia.

Extended geographical jurisdiction applies to each of these terrorism offences. This means that the offences can encompass activity that occurs outside Australia.

The Association Offence

The association offence has caused much concern. It is often misunderstood as having a much broader scope than it actually has. Often clients are unaware that the association must be for the purposes of providing support to a listed terrorist organisation. People also frequently do not realise that the association must be intentional and that there must be a certain level of knowledge involved.

Case Study:

Sylvia has been having meetings with Phillip, who is a member of Organisation X. Organisation X is an international organisation that has branches in Australia and in Indonesia. The Indonesian branch has been listed as a terrorist organisation. Phillip is a member of Organisation X in both Australia and Indonesia. He spends half of every year in Indonesia working for Organisation X there and the other half of each year working for the Australian branch. Sylvia has been meeting with Phillip to discuss ways in which Sylvia might assist in Organisation X's fundraising activities in Australia. Sylvia knows that Organisation X in Indonesia has been listed as a terrorist organisation in Australia although she is not aware that Organisation X in Australia is a branch of the Indonesian Organisation X. Sylvia's brother is also a member of Organisation X in Australia. Sylvia sees her brother once every few weeks at family gatherings but they have never discussed Organisation X at these events. Has Sylvia committed the association offence?

It is possible that Sylvia has committed the association offence in her dealings with Phillip. Her meetings with Phillip have occurred on more than one occasion and presumably she knew that Phillip was a member of Organisation X (as that was why she was meeting with him). Furthermore, the purpose of Sylvia's meetings with Phillip was to support Organisation X and she intended to help it carry on its activities by assisting with its fundraising. In determining if Sylvia has committed the offence, the key question that must be answered is whether Organisation X's Australian branch has been included in the listing of Organisation X's Indonesian branch. Whether Sylvia has offended will also depend on whether she was aware that Organisation X's Australian branch is a terrorist organisation under the Criminal Code definition (because of its links with Organisation X in Indonesia). If she did know these things then it is likely that Sylvia has committed the association offence.

In respect of Sylvia's associations with her brother, Sylvia will not have committed the association offence, regardless of the listing status of Organisation X's Australian branch. Their associations would fall within the exception for close family members, particularly as they have only been meeting at family functions and have never discussed Organisation X's activities at all. If Sylvia and her brother had met in a non-family-related situation for the purpose of discussing Organisation X, the exception would probably not apply.

Funding Terrorist Organisations

The offence of funding terrorist organisations has also caused a great deal of concern at a community level. This is because the offence may be committed by direct or indirect funding and also recklessly. This raises the possibility that persons donating to charitable organisations may commit the offence without intending to. Furthermore, the offence does not require that the funds be connected to a terrorist act or terroristic intention.

Case Study:

X asks Y to help her raise money for victims of an earthquake in Pakistan. Y helps X to raise funds. X then gives the funds to an organisation in Pakistan that, as well as helping with the earthquake, also engages in activities that would be regarded as fostering a terrorist act. Y knows that X is passing the funds on to that particular organisation but she does not know anything about the activities of the organisation. Is Y guilty of a funding offence?

Y may be guilty of the funding offence through recklessness. To make out a charge, the prosecution would need to prove beyond a reasonable doubt that Y *was reckless as to the circumstance* that the organisation to which her funds were going was a terrorist one. That is, that Y was aware of a substantial risk that the funds could have been given by X to a terrorist organisation. To be liable, it would need to be unjustifiable for Y, knowing all the circumstances and being aware of a *substantial risk*, to take that risk. It doesn't matter that Y was providing the funds to the terrorist organisation indirectly. The state of mind of Y is the most important thing.

The Attorney-General's Department has stated the following about the funding offence:

For the ordinary person who, for example, gives funds to a person believing that person is legitimately collecting money for charity or who collects funds believing that they are doing that for a legitimate charity, they will not commit an offence, *irrespective of where those funds are eventually used.*

Attorney-General's Department, quoted in Report of Senate Legal and Constitutional Committee: Provision of Anti-Terrorism Bill (No. 2) 2005

As noted above, the question of whether taking a risk is unjustifiable is a question of fact. As discussed above in relation to the concept of 'recklessness', a situation would need to be something in the order of an emergency for it to be justifiable to take the risk of funding a terrorist organisation (where one is aware that there is a substantial risk that this will occur).

The offence of funding terrorist organisations ...may be committed by direct or indirect funding and also recklessly.

ADVICE: steps clients may take to reduce risk when funding charities:

- Make *reasonable* enquiries. Find out from credible sources what the purpose of the funds is and who they are going to, including who might be the final recipient.
- Keep written records of these enquiries, including the date, who was spoken to, the information derived, and so on.
- Take steps to make sure that the recipient organisation is not one of the 19 listed terrorist organisations or part of one of those organisations or connected to one of those organisations. In particular, it is important to ascertain whether the recipient organisation might forward some of its funds to one of the listed terrorist organisations. It is important also to look at lawful ways the funds might be forwarded, such as through fees, levies, taxes or welfare provision.
- Take steps to find out the activities of the recipient organisation(s) to ensure that they are not engaged in preparing, planning, assisting in or fostering terrorist acts.
- Take steps to check whether the organisation is on the 'Consolidated List' of terrorist organisations. This is a list of 500+ organisations that have been classified by the United Nations as terrorist organisations. Obviously not all of these organisations have been listed in Australia, but it is still an offence to fund these organisations or deal with their assets. This list is available from the Department of Foreign Affairs and Trade website at <http://www.dfat.gov.au/icat/freezing_terrorist_assets.html>.
- As a result of such steps, the client should be satisfied that there is no risk that the funds will end up with an organisation that falls within the definition of a terrorist organisation.



FINANCING TERRORISM

Sections 103.1, 103.2, Part 5.3, Criminal Code

There are two offences that relate to financing terrorism. These are distinct from the offence of getting funds to or from a terrorist organisation (see page 8).

Financing terrorism

It is an offence to intentionally provide or collect funds while being reckless as to whether the funds will be used to facilitate or engage in a terrorist act (maximum penalty: life imprisonment).

It is an offence to intentionally provide or collect funds while being reckless as to whether the funds will be used to facilitate or engage in a terrorist act...

Financing a terrorist

It is an offence to intentionally:

- make funds available to another person (directly or indirectly) OR
- collect funds for, or on behalf of, another person (directly or indirectly)

while being reckless as to whether the funds will be used by that other person to facilitate or engage in a terrorist act. (maximum penalty: life imprisonment)

These offences may be committed even if:

- a terrorist act does not occur; OR
- the funds will not be used to facilitate or engage in a specific terrorist act; OR
- the funds will be used to facilitate or engage in more than one terrorist act.

Extended geographical jurisdiction applies to each of these terrorism offences. This means that offences encompass terrorist acts and offences that occur outside Australia.

Case Study:

Susan is asked to donate money to Organisation X, a charitable organisation in Australia. Organisation X sends most of the money it collects to Organisation Y in Country A. Organisation Y uses money it receives to, among other things, maintain its military wing, which is involved in armed warfare against the government of Country A. Susan is aware that Organisation X does send money to Organisation Y. She is not, however, aware of what Organisation Y does with that money. Would Susan have committed a financing offence by donating to Organisation X?

If Susan is aware of the fact that Organisation Y has a military wing that is involved in armed warfare against the government of Country A, in all likelihood she would have committed a financing offence. Organisation Y's military activities would clearly constitute terrorist acts. If Susan is aware that Organisation X is sending money to Organisation Y and if she is aware of Organisation Y's activities, she would have enough knowledge to be aware of a 'substantial risk' that the money she is donating will be used to fund or facilitate a terrorist act.

On the other hand, if Susan is not aware that Organisation Y has a military wing, then in all likelihood she would not have committed a criminal offence. While she would be aware of a substantial risk that the funds would be passed on to Organisation Y, she would not be aware of a substantial risk that the funds would be used to engage in or facilitate a terrorist act.

In any event, the precautionary measures relating to charitable donations as detailed above in relation to terrorist organisation offences should always be taken. It is better for clients to avoid taking such risks in the first place, than to claim ignorance afterwards.

It is also important to recall that in reality the majority of people making charitable donations will not be scrutinised by the authorities. We have seen that at different times certain ethnic and religious groups are more likely to be subject to scrutiny than others. Regrettably, it may be that members of ethnic and religious groups that are more likely to come under official scrutiny should be advised to take more comprehensive precautionary measures, as detailed on page 12.

...the precautionary measures relating to charitable donations should always be taken. It is better for clients to avoid taking such risks in the first place, than to claim ignorance afterwards.



ASIO AND THE AFP

There are two main organisations empowered in relation to counter-terrorism:

- Australian Security Intelligence Organisation (ASIO): This organisation gathers information relating to security. ASIO officers can question people to gather intelligence and can detain people for questioning, but they are not responsible for enforcing the anti-terrorism laws and cannot arrest people.
- Australian Federal Police (AFP): They investigate federal crimes like the terrorism offences. They have general police powers of search, arrest and detention.

ASIO officers can question people to gather intelligence and can detain people for questioning, but they are not responsible for enforcing the anti-terrorism laws and cannot arrest people.

Sometimes ASIO and the AFP work together. For example, the AFP may take someone into detention for questioning by ASIO or ASIO may ask for the AFP's help in gaining entry to premises to conduct a search. More recently there also seems to be greater information-sharing between ASIO and the AFP. This is significant for clients in that information gathered by ASIO may be passed on to the AFP. It may then form the basis for criminal investigation, arrest and prosecution.



ASIO's POWERS

ASIO's role in relation to terrorism offences

The principal functions of ASIO are detailed in section 17 of the *Australian Security Intelligence Organisation Act 1979* (Cth) ('the ASIO Act'). These include:

- to obtain, correlate and evaluate intelligence relevant to security;
- for purposes relevant to security... to communicate any such intelligence to such persons... as are appropriate to those purposes.

'Security' is defined as including:

- the protection of, and of the people of, the Commonwealth and the several States and Territories from (among other things) politically motivated violence; and
- the carrying out of Australia's responsibilities to any foreign country in relation thereto.

(These parts of the definition of 'security' are the most significant in relation to the anti-terrorism laws.)

The definition of 'politically motivated violence' explicitly includes terrorism offences (See section 4 of the ASIO Act, definition of 'politically motivated violence'). So it is within the scope of ASIO's functions to obtain, correlate and evaluate intelligence

relevant to terrorism offences, where these pose a threat to Australia or its people, or fall within the scope of Australia's responsibilities to a foreign country. More generally, politically motivated violence also means:

- acts or threats of violence or unlawful harm that are intended or likely to achieve a political objective, whether in Australia or elsewhere, including acts or threats carried on for the purpose of influencing the policy or acts of a government, whether in Australia or overseas; OR
- acts that involve violence or are intended or are likely to involve or lead to violence (whether by the persons who carry on those acts or by other persons) AND are directed to overthrowing or destroying or assisting the overthrow or destruction of the government or the constitution, both State or Federal.

'Terrorism offence' means an offence against Division 72 (terrorist bombings) or an offence under Part 5.3 of the Criminal Code (terrorism, terrorism organisation and financing terrorism offences).

'Security' is defined as including the protection of, and of the people of, the Commonwealth and the several States and Territories from (among other things) politically motivated violence.

Attorney General's Guidelines in relation to ASIO's performance of its functions

Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining intelligence relevant to security (including politically motivated violence)

As required by section 8A(1) of the ASIO Act, the Attorney-General has provided the Director-General of ASIO with guidelines on ASIO's performance of its function of obtaining intelligence relevant to security, including politically motivated violence ('the Guidelines'). New Guidelines were issued by the Attorney-General in October 2007.

The Guidelines identify that ASIO's functions require it to:

- a) undertake inquiries to determine whether a particular subject or activity is relevant to security;
- b) investigate subjects and activities relevant to security;
- c) develop and maintain a broad understanding of the security environment; and
- d) analyse and assess information obtained and to provide intelligence and advice to relevant authorities.

The Guidelines state that ASIO is not required to investigate every case of activities relevant to security. Rather, decisions on whether to initiate investigations should be based on a consideration of the likelihood of harm or damage from the subject's activities, ASIO's overall priorities and the availability of resources.

In deciding whether to conduct an investigation and determining what investigative methods to use, ASIO are required to consider the following:

- a) what is already known about the subject's activities, associates and beliefs, and the extent to which they are likely to be relevant to or prejudicial to security;
- b) the immediacy and severity of the threat to security;
- c) the reliability of the sources of the relevant information; and
- d) the investigative techniques that are likely to be most effective.

...decisions on whether to initiate investigations should be based on a consideration of the likelihood of harm or damage from the subject's activities, ASIO's overall priorities and the availability of resources.

In terms of the conduct of investigations, the Guidelines indicate the following (among other things):

- Intelligence relevant to security is to be obtained by ASIO in a lawful, timely and efficient way.

- There should be as little intrusion into individual privacy as possible, consistent with the performance of ASIO's functions.
- Investigations should be conducted with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest.
- Any means used to obtain information must be proportionate to the gravity of the threat to security posed and the likelihood of its occurrence.
- Wherever possible the least intrusive methods of information collection should be used before more intrusive techniques.
- Where a threat is assessed as likely to develop quickly, a great degree of intrusion may be justified.

The Guidelines address the issue of ASIO's treatment of personal information. They provide that ASIO must only collect, use, handle or disclose personal information for purposes connected with its statutory functions. They also provide that ASIO must keep appropriate records of all requests that they make for access to personal information and all communications of personal information that they make. These records must be open to inspection by the Inspector-General of Intelligence and Security (see page 46).

ASIO investigations must be reviewed annually by ASIO. Furthermore, ASIO is required to keep the Attorney-General advised of its investigations and priorities by regular briefings.

As required by section 8A(2) of the ASIO Act, the Guidelines also address ASIO's performance of its functions that relate to politically motivated violence.

...the ASIO Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not by itself be regarded as prejudicial to security...

The Guidelines refer to section 17A of the ASIO Act, which provides that the ASIO Act 'shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not by itself be regarded as prejudicial to security, and functions of [ASIO] shall be construed accordingly.'

The definition of politically motivated violence relied on in the Guidelines is the same as that contained in the ASIO Act (as detailed on page 16). Further, the Guidelines state that when performing its functions in relation to politically motivated violence, ASIO should give priority to people or groups aiming to achieve a political objective through:

- a) act or threats of serious violence or unlawful harm designed to create fear or to incite or provoke violent reactions; or
- b) the use of tactics that can reasonably be assessed as likely to result in violence.

The Guidelines point out that a person or group need not intend to initiate violence for the purpose of overthrowing the government. Their activities may still be considered

politically motivated violence if there is a 'reasonable likelihood' that their activities will cause others to be violent.

Similarly, the Guidelines state that advocacy of violence may fall within the definition of politically motivated violence, even where that advocacy is not public.

In relation to 'apparently non-violent activities' directed at destabilising or undermining the government, the Guidelines state that ASIO may investigate those activities to the extent necessary to establish whether there is a real risk that violence will flow from the activities. For ASIO to investigate them, these non-violent activities must be associated with a contemplation of the prospect of violent overthrow of the government.

The Guidelines expressly state that ASIO is not to undertake investigations where the only basis for the investigation is the exercise of a person's right of lawful advocacy, protest or dissent.

The Guidelines state that ASIO is not to make inquiries into demonstrations or other protest activity unless:

- There is a risk of premeditated violence against people or property for the purpose of achieving a political objective; or premeditated use of tactics that can be reasonably assessed as likely to result in violence; OR
- ASIO suspects that there is a link between the demonstration or other protest activity and conduct otherwise coming within the definition of security.

The Guidelines do provide an exception to this: ASIO can investigate demonstrations and protests that relate to internationally protected persons or other persons specified by the Attorney-General.

The Guidelines acknowledge that there may at times be some overlap between police and ASIO areas of responsibility. They provide that minor acts of violence such as jostling or defacing/damaging property are matters for investigation by police. Similarly, incidental acts of violence or property damage that occur in the course of a demonstration are also properly matters for the police to deal with. The Guidelines state, however, that where such acts are intended to be part of a pattern and are intended to influence the policy or action of government, ASIO may investigate to determine whether there is a potential for the violence to escalate or become more strongly directed at an associated person or group.

Requesting information from carriers

Section 23, ASIO Act

ASIO may, for the purpose of carrying out its functions, question aircraft or vessel operators about their cargo, crew, passengers, stores or voyage, and may demand production of documents under an operator's control relating to such matters. It is a strict liability offence to fail to answer such a question or to fail to produce a requested document, although a defence of reasonable excuse applies.

Special powers warrants

Division 2, Part III, ASIO Act

ASIO may also be issued with a variety of warrants. 'Special powers' warrants are issued by the Attorney-General at the request of the head of ASIO, who is known as the Director-General of Security. The Director-General must specify the grounds that make it necessary to issue the warrant, and must report in writing the extent to which action taken under the warrant assisted ASIO to carry out its functions. If, while a warrant is still in force, the Director-General becomes satisfied that these grounds have ceased to exist, s/he must inform the Attorney-General and take the necessary steps to ensure that activity under the warrant (other than recovering listening or tracking devices) is discontinued.

The following categories of warrant may be issued:

- search warrants
- computer access warrants
- listening device warrants
- tracking device warrants
- postal inspection warrants
- delivery service inspection warrants.

'Special powers' warrants are issued by the Attorney-General at the request of the head of ASIO.

Search warrants

Section 25, ASIO Act

The Attorney-General may issue an ASIO search warrant only if satisfied that there are reasonable grounds for believing that access by ASIO to records or things on the premises to be searched will substantially assist the collection of intelligence in respect of a matter that is important to security. The warrant must come into force within 28 days, and may stay in force for up to 90 days.

The warrant must specify the premises to be searched and times that entry is authorised. A warrant may authorise:

- entering the premises;
- searching the premises for records or things relevant to the security matter in relation to which the warrant was issued (including parcels or containers where there is reasonable cause to think relevant things will be found therein);
- searches (but not strip or cavity searches) of persons at or near the premises when the warrant is executed, if there is reasonable cause to believe that they have on their person relevant records or things;
- inspecting and examining any such record or thing that is found, and making copies or transcripts of records or things that appear relevant to the collection of intelligence in accordance with the Act;

- removing any such record or thing that is found, for the purposes of inspection, examination, copying or transcribing – anything that is removed may be retained if its return would be prejudicial to security, or otherwise for such time as is reasonable;
- if there is reasonable cause to believe that relevant data is on a computer, data storage device (e.g. disk or memory stick) or other electronic equipment, the use of that equipment to obtain that data, inspect and examine it, copy it, and/or print it out; and
- doing anything reasonably necessary to conceal the fact that the warrant has been executed.

The warrant must authorise the use of such force as is necessary and reasonable for the purposes of the search.

In practice, subjects of such search warrants may not always be given a copy of the warrant. Rather, they may receive a general information sheet that explains that a warrant has been issued and what it allows.

Where items are taken away by ASIO under a search warrant, the occupier should make sure s/he receives a receipt clearly identifying all items taken.

The warrant must authorise the use of such force as is necessary and reasonable for the purposes of the search.

Computer access warrants

Section 25A, ASIO Act

The Attorney-General may issue an ASIO computer access warrant only if satisfied that there are reasonable grounds for believing that access by ASIO to data held in the target computer will substantially assist the collection of intelligence in respect of a matter that is important to security. The warrant may stay in force for up to 6 months.

The warrant may authorise:

- entering specified premises;
- using a computer, a data storage device, a telecommunications facility or any other electronic equipment to obtain access to relevant data stored in the target computer;
- copying any data that is obtained and that appears relevant to the collection of intelligence;
- doing anything reasonably necessary to conceal the fact that the warrant has been executed.

The warrant must authorise the use of such force as is necessary and reasonable to do the things that it authorises, and must specify at what time(s) entry is authorised.

Listening device warrants

Section 26, ASIO Act

Listening device warrants may pertain to a particular person or to particular premises.

Listening device warrants may pertain to a particular person or to particular premises.

The Attorney-General may issue an ASIO listening device warrant in respect of a particular person only if satisfied that:

- a person is engaged in activities prejudicial to security, or is reasonably suspected by the Director-General of being engaged in, or being likely to engage in, such activity; and
- the use by ASIO of a listening device to listen to or record that person's communications will, or is likely to, assist ASIO to obtain intelligence relevant to security.
- The warrant will authorise
 - using a device to listen or record the person's communications;
 - entering any premises where the person is or is likely to be in order to install, use or maintain a listening device;
 - entering any other premises specified in the warrant from which the person's communication can be listened to or recorded, in order to install, use or maintain a listening device;
- the use of such force as is necessary and reasonable to do the things that the warrant authorises.

The warrant must specify at what time(s) entry is authorised.

The Attorney-General may issue an ASIO listening device warrant in respect of particular premises only if satisfied that:

- the premises are used, likely to be used or frequented by a person engaged in activities prejudicial to security, or reasonably suspected by the Director-General of being engaged in, or being likely to engage in, such activity; and
- the use by ASIO of a listening device to listen to or record communications to or from those premises will, or is likely to, assist ASIO to obtain intelligence relevant to security.

The warrant will authorise:

- using a device to listen to or record communications to or from anyone on the premises;
- entering the premises in order to install, use or maintain a listening device;
- entering any other premises specified in the warrant from which communications to or from the premises can be listened to or recorded, in order to install, use or maintain a listening device;
- the use of such force as is necessary and reasonable to do the things that the warrant authorises.

The warrant must specify at what time(s) entry is authorised.

A listening device warrant may remain in force for up to 6 months. ASIO may also enter premises, using such force as is reasonable and necessary, to recover a listening device installed pursuant to a warrant, even after the warrant has expired.

Without a warrant, it is unlawful for an ASIO officer or operative to use a listening device to listen to or record a communication unless the communicating person intends, or should reasonably expect, the officer or operative to be among those to whom the communication is made, or s/he consents.

A listening device warrant may not authorise interception of telecommunications.

Tracking device warrants

Section 26A, ASIO Act

The Attorney-General may issue an ASIO tracking device warrant only if satisfied that:

- a person, who is specified in the warrant, is engaged in activities prejudicial to security, or is reasonably suspected by the Director-General of being engaged in, or being likely to engage in, such activity, and applying a tracking device to an object (e.g. vehicle, aircraft, vessel, clothing) likely to be used or worn by the person will, or is likely to, assist ASIO in obtaining intelligence relevant to security; OR
- a particular object specified in the warrant is likely to be used or worn by a person (identified or unidentified) who is engaged in activities prejudicial to security, or is reasonably suspected by the Director-General of being engaged in, or being likely to engage in, such activity, and applying a tracking device to that object will, or is likely to, assist ASIO in obtaining intelligence relevant to security.

The warrant must authorise applying a tracking device either to a relevant object for the tracking of the specified person, or to the specified object so that it can be tracked.

The warrant may authorise:

- applying and/or maintaining a tracking device;
- entering premises where a target object is or is likely to be found, in order to apply, use or maintain a tracking device (if the warrant specifies an object rather than a person, the premises must be specified in the warrant);
- entering or altering an object in order to apply, maintain or use a tracking device.

The warrant must authorise applying a tracking device either to a relevant object for the tracking of the specified person, or to the specified object so that it can be tracked.

The warrant will authorise the use of such force as is necessary and reasonable to do the things it authorises. It must also specify at what time(s) entry is authorised.

The warrant may remain in force for up to 6 months. ASIO may also enter premises where a target object is or is likely to be found, or enter or alter a target object, using such force

as is reasonable and necessary to recover a tracking device installed pursuant to a warrant. They may do this even after the warrant has expired.

Without a warrant, it is unlawful for an ASIO officer or operative to use a tracking device to track a person or object (e.g. vehicle, aircraft, vessel, clothing) unless the person, or the person using the object, consents.

Postal and delivery service inspection warrants

Section 27, ASIO Act

The Attorney-General may issue an ASIO postal inspection warrant, and/or an ASIO delivery service inspection warrant, in respect of a particular person, only if:

- the person is engaged in activities prejudicial to security, or is reasonably suspected by the Director-General of being engaged in, or being likely to engage in, such activity; AND
- access by ASIO to articles posted by or to the person while in the course of the post, or sent by or to the person via a delivery service while being delivered, will, or is likely to, assist ASIO in obtaining intelligence relevant to security.

The warrant may authorise inspection and copying of the covers of articles, and opening the articles and inspecting and copying their contents.

The Attorney-General may issue an ASIO postal inspection warrant, and/or an ASIO delivery service inspection warrant, in respect of a particular address, only if

- some or all of the postal or delivery service articles for that address are to be received by a person (identified or unidentified) who is engaged in activities prejudicial to security, or is reasonably suspected by the Director-General of being engaged in, or being likely to engage in, such activity; AND
- access by ASIO to articles posted or sent to the address will, or is likely to, assist ASIO in obtaining intelligence relevant to security.

The warrant may authorise inspection and copying of the covers of articles, and opening the articles and inspecting and copying their contents if they appear to be, or are reasonably suspected of being, intended for the relevant person.

The warrant may remain in force for up to 6 months.

Without a warrant, it is unlawful for ASIO to seek, or be given, access to a postal or delivery service article, or information about its contents or cover, unless it is a postal article addressed to, or intended to be received by, ASIO.

*Without a warrant,
it is unlawful for
an ASIO officer or
operative to use a
listening device to
listen to or record a
communication...*

Foreign intelligence warrants

Section 27A, ASIO Act

Warrants may also be issued authorising ASIO to undertake any of the above investigative activities in order to obtain intelligence relating to the capabilities, intentions or activities of a foreign government or political organisation. (See section 4 of the ASIO Act, definition of 'foreign intelligence' and 'foreign power'.) Such warrants may not be requested for the purpose of collecting information about Australian citizens or permanent residents. In other respects these warrants conform to the constraints of those already discussed.

Although the collection of foreign intelligence does not fall under the definition of 'security' in the ASIO Act, these warrants may still be relevant to the investigation of certain terrorism offences.

Other aspects of the special powers warrants regime

There are no constraints on the Attorney-General issuing repeat warrants.

In certain circumstances, the Director-General may issue a warrant him/herself:

- The Director-General must have requested that the Attorney-General issue the warrant.
- To the knowledge of the Director-General, the Attorney-General must not have refused the request.
- The Attorney-General must not have refused a substantially similar warrant in the past 3 months.
- The Director-General must not have issued a substantially similar warrant in the past 3 months.
- The Director-General must be satisfied that the facts of the case would justify the Attorney-General issuing the warrant.
- The Director-General must be satisfied that security will be, or is likely to be, seriously prejudiced by not doing what the warrant would authorise before the Attorney-General can issue it.

Warrants may also be issued authorising ASIO to... obtain intelligence relating to the capabilities, intentions or activities of a foreign government or political organisation.

The Director-General must provide a copy of the warrant to both the Attorney-General and the Inspector-General of Intelligence and Security (see page 46 for more information regarding this office). The Attorney-General must also be provided with a statement of the grounds on which the Director-General is satisfied of the last-mentioned matter above (that is, the emergency need for the warrant). Such a warrant remains in force for no more than 2 days. The Director-General may not issue a foreign intelligence warrant, even in an emergency.

The Attorney-General may always revoke a warrant before its period expires.

Telecommunications Interception Warrants

Telecommunications (Interception and Access) Act 1979 (Cth)

These warrants are governed by the *Telecommunications (Interception and Access) Act 1979 (Cth)* ('the TIA Act'), rather than the ASIO Act, but in most respects are similar to the ASIO Act's special powers warrants.

In general, it is unlawful for ASIO to intercept telecommunications, unless this occurs in the course of discovering the location of a listening device.

The Attorney-General may issue a warrant authorising ASIO to intercept a particular telecommunications service upon a request by the Director-General of Security, which sets out the grounds on which the warrant is sought. The Attorney-General must be satisfied that:

- the telecommunications service in question is being, or is likely to be, used by a person who is engaged in activities prejudicial to security, or is reasonably suspected by the Director-General of being engaged in, or being likely to engage in, such activity, or is the means by which someone communicates with such a person – in this case the Attorney-General must also be satisfied either that ASIO has tried all other practicable methods of identifying the latter person's own telecommunication service, or that it would not be possible to intercept communications from that service – or is used for purposes prejudicial to security; AND
- the intercepted telecommunications will, or are likely to, assist ASIO in obtaining intelligence relevant to security.

The Attorney-General may issue a warrant authorising ASIO to intercept the telecommunications from any service, or particular device, that a particular person is likely to use upon a request by the Director-General of Security. The Attorney-General must be satisfied that:

- the person is engaged in activities prejudicial to security, or is reasonably suspected by the Director-General of being engaged in, or being likely to engage in, such activity; AND
- the intercepted telecommunications will, or are likely to, assist ASIO in obtaining intelligence relevant to security; AND
- if the warrant pertains to a particular device, there are no other practicable methods of identifying the person's telecommunications service, or that it would not be practicable to intercept communications from that service; AND
- the first sort of warrant mentioned above would be ineffective for obtaining the intelligence.

In addition to authorising interception, the warrant authorises access to stored communications (e.g. voicemail or email) and may also authorise entry to premises in order to use, maintain, install or recover interception equipment. In the latter case, the warrant must specify at what time(s) entry may take place, and whether or not permission must first be sought.

Generally, a warrant remains in force for up to 6 months. If a warrant is issued in relation to a service that is the means by which the target person is likely to be communicated with, it remains in force for up to 3 months. Repeat warrants are not precluded. The Attorney-General may revoke a warrant before it expires. As with the special powers warrants, the Director-General must report in writing the extent to which action taken under the warrant assisted ASIO to carry out its functions. If, while a warrant is still in force, the Director-General becomes satisfied that the grounds on which it was issued have ceased to exist, s/he must inform the Attorney-General and take the necessary steps to ensure that activity under the warrant is discontinued.

As with the special powers warrants, and subject to the same constraints, the Director-General may issue a warrant him/herself, with such a warrant remaining in force for 2 days. There is also provision for telecommunications interception warrants pertaining to foreign intelligence.

Security Assessments

Division 1, Part IV, ASIO Act

Under the ASIO Act, a further function of ASIO is to provide security assessments to Commonwealth, State and Territory governments.

Security assessments may be required in a range of circumstances. One common circumstance is visa applicants: under the Migration Regulations 1994 (Cth), the majority of applicants must satisfy 'public interest criterion 4002' before a visa may be issued. This criterion is set out in Schedule 4, Part 1 of the Migration Regulations as follows:

The applicant is not assessed by the Australian Security Intelligence Organisation to be directly or indirectly a risk to security, within the meaning of section 4 of the *Australian Security Intelligence Organisation Act 1979*.

Many jobs in government agencies also require security clearances. Also, under the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), in certain circumstances it can become necessary for lawyers to seek security clearances if they are to act in certain matters (see sections 29(3), 38I(3), 39, 39A, 46, 46G in that Act).

Part IV, Division 2 of the ASIO Act establishes certain rights in respect of a person who is given a qualified or adverse security assessment. It is important to note, however, that these rights do not extend to a person who is not an Australian citizen, who does not hold a valid permanent visa, and who is being assessed under the Migration Regulations. (See section 36(b) and the definition of 'prescribed administrative action' in section 35.)

Under the ASIO Act, a further function of ASIO is to provide security assessments to Commonwealth, State and Territory governments.

Questioning People

Under the anti-terrorism legislation ASIO has increased powers to question and detain people in relation to terrorism offences. These powers arise from Division 3 of the ASIO Act.

Questioning People without a Warrant

ASIO can question people without a warrant as long as they consent. In practice, ASIO will often contact a person they wish to get information from and ask them for an informal chat. It has been reported by community members that ASIO may also suggest to such a person that they can 'do this the easy way or the hard way'. That is, that they could get a questioning warrant, but it would be easier if the person just chatted to them without it. When a complaint about this conduct was made to the Inspector-General of Intelligence and Security (see page 46), ASIO denied that they approach people in this way. In the case of *R v Ul-Haq [2007] NSWSC 1251*, however, ASIO officers themselves gave evidence about using words to the effect that 'we can go down the difficult path or a less difficult path'. ASIO were heavily criticised by the Court for their questioning tactics. In particular, the Court found that ASIO had not made it clear to Mr Ul-Haq that he was under no obligation to speak to them and furthermore, that they had used coercive and intimidating interrogation techniques. In that case, ASIO officers questioned Mr Ul-Haq without a questioning warrant while other ASIO officers were executing a search warrant at his house. The Court even indicated that the ASIO officers involved had in all likelihood committed the crime and/or tort of false imprisonment.

If ASIO does approach someone for an informal interview, that person is under no obligation to speak to ASIO. It may, however, be the case that if the person does not cooperate, ASIO will obtain a questioning warrant in order to question him or her. The grounds for obtaining a questioning warrant are detailed on pages 30-31.

Any information a person gives to ASIO, even in an informal interview, may be used against that person or their friends or family later on. For example, the information may be passed on to the AFP to aid in the investigation of a criminal offence.

Clients may feel reluctant to refuse to speak with ASIO, particularly if they believe they have not committed any offence and therefore have nothing to hide. It is generally best, however, to advise clients to tell ASIO that they will 'think about it' and then to contact a lawyer for advice before participating in an interview. Clients may not realise the breadth of Australia's anti-terrorism laws and they may not be fully aware of how information they give to ASIO can be used.

Under the anti-terrorism legislation ASIO has increased powers to question and detain people in relation to terrorism offences.

Lawyers advising clients who have been contacted by ASIO should try to ascertain the following before giving advice:

- any links the client may have to terrorist organisations (listed or otherwise);
- any financial transactions the client has made that may relate to terrorist acts or organisations, in Australia or overseas;
- whether the client has any connections that may have led him/her to have information about terrorist acts or organisations, in Australia or overseas;
- whether the client is in possession of any documents or electronic records that may be incriminating;
- whether the client is in possession of any material that has been associated with terrorist acts, such as so-called extremist literature;
- whether the client tends to visit websites on the internet that may suggest an involvement in, interest in or possession of information about terrorist acts or organisations;
- whether the client has been overseas in recent times to any countries in which terrorist organisations are based (listed or otherwise);
- any other information that may explain why ASIO would like to interview the client.

Once as much information as possible has been obtained, a client should be advised if there is a possibility that ASIO could get a questioning warrant (see pages 30-31). A client should also be advised about any possibility of criminal charges and about any possibility that material and records s/he possesses may be incriminating.

A client should also be advised about the Attorney-General's Guidelines relating to ASIO's investigations and about the Inspector-General of Intelligence and Security (see page 46).

Unfortunately, ASIO will not usually consent to the person having a lawyer present during these informal interviews unless that lawyer has security clearance. ASIO may, however, consent to a family member of the subject being present depending on the circumstances.

Questioning Warrants and Questioning and Detention Warrants

Division 3, Part III, ASIO Act

Division 3 of Part III of the ASIO Act gives ASIO the power, subject to warrant, to question and detain people suspected of having intelligence relevant to a terrorism offence.

The basics: what a warrant authorises

Sections 34E and 34G, ASIO Act

There are two sorts of warrants – questioning warrants (issued under section 34E), and questioning and detention warrants (issued under section 34G):

- A questioning warrant requires the subject to appear before a prescribed authority for questioning, either immediately, or at a time specified in the warrant.
- A questioning and detention warrant authorises the subject to be taken immediately into custody by a police officer, to be brought immediately before a prescribed authority for questioning, and to be detained by police.
- These warrants authorise ASIO to question the person before a 'prescribed authority' by requiring the person to
 - give information that is or may be relevant to intelligence that is important in relation to a terrorism offence; AND/OR
 - produce records or things that are or may be relevant to intelligence that is important in relation to a terrorism offence.

Such warrants also authorise ASIO to make copies and/or transcripts of records produced in response to a request.

The person authorised to exercise authority under the warrant will typically be an officer of ASIO, but may be another person so authorised by the Director-General (section 24).

Issuing a warrant

Sections 34D and 34F, ASIO Act

The process by which a warrant is issued is complicated. The first step must be taken by the Director-General of Security.

- The Director-General must present a draft warrant to the Attorney-General, and seek his/her consent to a request that a warrant be issued.
- The request must be accompanied by a statement of the grounds that make the warrant necessary.

Next, the Attorney-General must decide whether or not to allow the Director-General to request the warrant. The Attorney-General may consent only if satisfied:

- that there are reasonable grounds for believing that issuing the warrant will substantially assist the collection of intelligence that is important in relation to a terrorism offence; AND
- that relying on other methods of collecting that intelligence would be ineffective.

There are two sorts of warrants – questioning warrants, and questioning and detention warrants.

If the warrant to be requested is a questioning and detention warrant, the Attorney-General must also be satisfied that there are reasonable grounds for believing that, if the person is not detained, s/he may:

- alert someone involved in a terrorism offence that the offence is being investigated; OR
- not appear to be questioned; OR
- destroy, damage or alter a record or thing that may be requested pursuant to the warrant.

If the Attorney-General consents to the Director-General making the request, the Director-General may present the draft warrant, together with a copy of the Attorney-General's written consent, to an issuing authority and request a warrant.

- Under section 34AB an issuing authority is a federal magistrate or federal judge who has been appointed as such (to avoid constitutional difficulties s/he acts in a personal, not a judicial, capacity – see section 34ZM(2)).
- The issuing authority may issue the warrant only if s/he is satisfied that there are reasonable grounds for believing that the warrant will substantially assist the collection of intelligence that is important in relation to a terrorism offence.
- The issued warrant must be in the same terms as the draft warrant.
- The warrant may be in force for up to 28 days.

There is no requirement that the issuing authority be satisfied that relying on means other than a warrant for collecting the intelligence would be ineffective. Thus, this part of the process is all decided in house, between the Director-General and the Attorney-General (arguably making it a less effective constraint on the issuing of warrants).

Contact with a lawyer: what a warrant must permit

Sections 34D, 34E, and 34F, ASIO Act

The Attorney-General may consent to the Director-General requesting a warrant only if the warrant will permit the subject to contact a single lawyer of their choice:

- in the case of a questioning warrant, at any time they are appearing before a prescribed authority pursuant to the warrant;
- in the case of either sort of warrant, at any time they are detained pursuant to the warrant (how a questioning warrant may result in detention is explained at page 37).

The Attorney-General may consent to the Director-General of ASIO requesting a warrant only if the warrant will permit the subject to contact a single lawyer of their choice.

In the latter case, the warrant must permit the person to contact a lawyer only after they have:

- identified their lawyer to the prescribed authority; AND
- given ASIO the opportunity to request the exclusion of that lawyer.

The role of lawyers, and the basis on which ASIO can seek their exclusion, is explained below.

Repeat warrants – additional requirements

Sections 34D, 34F and 34G, ASIO Act

There are additional requirements where a warrant has previously been sought in relation to a person. When the Director-General presents the draft request to the Attorney-General:

- s/he must also state the outcomes of any previous requests for warrants to the same person;
- the draft request must detail any previous ASIO warrants of any type issued to the same person, including the duration of any questioning, and of any detention under a questioning and detention warrant.

There is, however, no statutory requirement that previous detention pursuant to a questioning warrant (as opposed to a questioning and detention warrant) be brought to the attention of the Attorney-General.

Then, if a questioning and detention warrant is being sought, and the person has already been detained pursuant to an ASIO warrant, the Attorney-General and the issuing authority must also:

- take account of the fact that any previous detention pursuant to an ASIO warrant has taken place; AND
- be satisfied that the issue of the warrant is justified by information that is additional to or materially different from that known to the Director-General at the time the Director-General sought the Attorney-General's consent to request the issue of the last of the earlier warrants.

The issuing authority must also be satisfied that the person is not being detained pursuant to one of those earlier warrants at that time.

In certain circumstances, repeat warrants are legal only where additional or materially different information comes into the possession of the Director-General. In practice, this could be difficult to confirm given the covert manner in which ASIO operates.

What if the grounds on which the warrant was issued cease to exist?

Section 34ZK, ASIO Act

If, before a warrant expires, the Director-General is satisfied that the grounds on which the warrant was issued have ceased to exist, s/he must inform the Attorney-General and the issuing authority, and take necessary steps to ensure that action under the warrant is discontinued.

Questioning before a prescribed authority and detention

Sections 34B, 34K, 34F, 34ZF, ASIO Act

A prescribed authority is a person appointed by the Attorney-General, either a retired judge of at least 5 years' experience, or a serving State judge of at least 5 years' experience, or a President or Deputy-President of the Administrative Appeals Tribunal who has been a registered legal practitioner for at least 5 years. It is the job of the prescribed authority to supervise ASIO's execution of the warrant.

The prescribed authority has the power to:

- issue directions about the arrangements for a person's detention;
- order the release of a person from detention;
- defer questioning; and
- direct a person's further appearance before a prescribed authority for questioning under the warrant.

It is the job of the prescribed authority to supervise ASIO's execution of the warrant.

The last two powers allow the prescribed authority to determine when, and for how long, questioning takes place. All detention must be by the police.

Anyone who knowingly contravenes a direction given by the prescribed authority, which they were responsible for implementing, is guilty of an offence (maximum penalty: 2 years' imprisonment).

Bringing a person before a prescribed authority

Sections 34F, 34L, 34U, 34V, 34ZF

A person who does not appear before a prescribed authority for questioning (whether as a warrant directs, or as a prescribed authority has directed pursuant to a warrant) commits an offence (maximum penalty: 5 years' imprisonment). A police officer may take such a person into custody and bring them before a prescribed authority for questioning.

Where the police are authorised to take someone into custody (either pursuant to a detention warrant or because the person has not appeared before a prescribed authority), they may enter premises using reasonable and necessary force. They may also use reasonable and necessary force to arrest the person.

A police officer who takes someone into custody pursuant to a questioning and detention warrant and knowingly fails to make arrangements immediately to bring them before a prescribed authority for questioning, commits an offence (maximum penalty: 2 years' imprisonment).

Searches

Sections 34NB, 34ZB, 34ZC and 34ZD, ASIO Act

If a person is detained, the police may subject them to an ordinary search (this also permits removal and examination of jacket, coat, gloves, shoes and hat) or a strip search.

A 'strip search' is defined as a search of the person's body with garments removed, and of his/her garments. A strip search does not include a search of a person's body cavities (see the section 4 definition of 'strip search' in the ASIO Act).

A strip search may take place only if:

- the person consents in writing; OR
- the police suspect on reasonable grounds that the person has on their body an item likely to pose a danger to someone, or to assist someone to escape, and that a strip search is the only way to recover the item.

The prescribed authority must approve the search and must make a record of the decision and the reasons for it.

Necessary and reasonable force may be used to conduct a strip search.

Any item found during a search that is likely to pose a danger to someone or to assist someone to escape may be seized and may be retained by the police for such time as is reasonable.

Any item relevant to collection of intelligence that is important in relation to a terrorism offence may be seized and may be retained by ASIO for as long as its return would be prejudicial to security, or otherwise for such time as is reasonable.

If a person's clothes are seized, the person must be provided with adequate clothing.

It is an offence for a police officer to knowingly violate the strip search rules (maximum penalty: 2 years' imprisonment).

Compulsory questioning

Section 34L, ASIO Act

A person before a prescribed authority for questioning who fails to provide information requested, or to produce any record or thing requested, commits an offence (maximum penalty: 5 years' imprisonment).

It is a defence to such an offence that the person does not have the information, record or thing. It is important to note that because of the way these offences are structured, to get a conviction the prosecution does not have to prove beyond reasonable doubt that the person knew the information or had the thing. They must only prove that the information

or thing was not handed over. If the accused wishes to run a defence of ignorance, or non-possession of the record or thing, they bear an evidentiary burden. This means that the accused must adduce evidence that suggests a reasonable possibility that they did not have the information, record or thing. The most obvious way of discharging this burden is for the accused to testify – but of course this requires the accused to waive his/her right to silence. Once the accused has discharged this evidentiary burden the onus is on the prosecution to prove beyond a reasonable doubt that the defence raised does not apply.

A person before a prescribed authority for questioning who fails to provide information requested, or to produce any record or thing requested, commits an offence.

It is an offence for a person to make a false or misleading statement during questioning under a warrant (maximum penalty: 5 years' imprisonment). It is a defence that the statement was not false or misleading in a material particular. Again, the accused bears an evidential burden in respect of this defence.

Video-recording

Sections 34K and 34ZA, ASIO Act

The Director-General must ensure that the person's questioning before a prescribed authority is video-recorded. S/he must also ensure the video-recording of anything else that the prescribed authority directs.

Inspection of items by ASIO

Section 34ZD, ASIO Act

ASIO has the power to inspect certain items produced during questioning and/or detention:

- ASIO may remove, inspect and examine any record or thing produced under questioning.
- ASIO may remove, and retain so as to make copies and/or transcripts in accordance with the warrant, any record produced under questioning.
- ASIO may examine any thing removed from the person in the conduct of a search.
- ASIO may make copies of items seized during searches on the basis that they are relevant to the collection of intelligence that is important in relation to a terrorism offence.

Anything taken by ASIO may be retained for as long as its return would be prejudicial to security or otherwise for such time as is reasonable.

Anything taken by ASIO may be retained for as long as its return would be prejudicial to security or otherwise for such time as is reasonable.

Destruction of records

Section 34ZL, ASIO Act

Where a record or copy was made because of a warrant and is in the possession of ASIO, if the Director-General is satisfied that it is not required for the performance of functions or exercise of powers under the ASIO Act, s/he may have it destroyed.

Restrictions or conditions imposed on ASIO by the warrant

Sections 34E, 34F and 34G, ASIO Act

A warrant may place restrictions or conditions on ASIO's questioning, and on the making of copies or transcripts of records produced in response to questioning. A person authorised to exercise authority under a warrant who knowingly contravenes a

restriction or condition in the warrant commits an offence (maximum penalty: 2 years' imprisonment).

Duration of questioning permitted

Sections 34R and 34ZF, ASIO Act

The questioning must end after 8 hours. It may, however, be extended by the prescribed authority upon a request by ASIO, for rolling 8-hour periods, up to a maximum of 24 hours (or 48 hours if a person is being questioned with an interpreter):

- An extension may be requested even if the person being questioned or their legal or other representative is not present.
- In extending the duration of questioning, the prescribed authority must be satisfied that there are reasonable grounds for believing that permitting questioning to continue will substantially assist the collection of intelligence that is important in relation to a terrorism offence, and that ASIO has been conducting the questioning of the person properly and without delay.
- The prescribed authority may revoke the extension.

It is an offence for an ASIO officer exercising authority under a warrant to knowingly question someone once the permissible time for questioning has expired (maximum penalty: 2 years' imprisonment).

If the prescribed authority defers questioning for one of the following reasons, the time that passes does not count against the limit on total questioning time:

- in order for recording equipment to be changed;
- in order for the person to contact a lawyer or other person, or to make a complaint (as discussed on page 39);
- in order for the person to rest, recuperate or receive medical attention;
- in order for the person to engage in religious practices;
- any other time, if the prescribed authority so determines.

It is an offence for an ASIO officer exercising authority under a warrant to knowingly question someone once the permissible time for questioning has expired.

Duration of detention permitted

Sections 34G, 34R and 34S, ASIO Act

If a person has been detained, s/he must be released once:

- ASIO tells the prescribed authority they have nothing more to ask the person; OR
- the time for questioning has ended (whether because the 24/48-hour limit has been reached or because the prescribed authority will not extend it or has revoked an extension); OR

- a week has passed since the person was first brought before a prescribed authority in accordance with the warrant; OR
- the person has been detained for a continuous period of a week (168 hours).

Detention without a detention warrant

Section 34K, ASIO Act

When a person is before a prescribed authority for questioning, that authority may give a direction to detain a person, even if the warrant is a questioning warrant and not a detention warrant. The prescribed authority may do this only if s/he is satisfied that there are reasonable grounds for believing that unless detained the person may:

- alert someone involved in a terrorism offence that the offence is being investigated; OR
- not continue to appear, or not appear again, to be questioned; OR
- destroy, damage, or alter a record or thing that has been, or may be, requested pursuant to the warrant.

Such detention is still subject to the limits described above. Detention must be by the police.

Basic right to humane treatment

Sections 34T, 34ZF

The ASIO Act provides that a person against whom a warrant has been issued must be treated with humanity and with respect for human dignity, and must not be subjected to cruel, inhuman or degrading treatment. Contravention of this requirement is an offence (maximum penalty: 2 years' imprisonment).

In addition, the ASIO Act requires ASIO to adopt a Protocol detailing the procedures to be followed in the exercise of authority under these warrants. This Protocol was adopted in August 2003. Some of its key elements are:

- Force and restraint may not be used to punish the person against whom the warrant has been issued, and only a police officer may apply restraint.
- Fresh drinking water must be available at all times and three meals a day supplied.
- When in detention, a minimum of 8 hours' continuous, uninterrupted sleeping time must be provided in each 24-hour period.
- Those present during questioning and detention must be humane and courteous and must not speak to the person against whom the warrant has been issued in a demeaning manner.

The ASIO Act provides that a person against whom a warrant has been issued must be treated with humanity and with respect for human dignity, and must not be subjected to cruel, inhuman or degrading treatment. Contravention of this requirement is an offence.

- A police officer must be present during questioning.
- Questioning is to be limited to 4-hour periods, with a minimum 30-minute break after any 4-hour period.
- If the video-recording equipment malfunctions during questioning or if recording has been suspended for some reason, questioning must stop until recording can be resumed.

Right to be informed upon being brought before the prescribed authority

Section 34J, ASIO Act

When a person first appears before the prescribed authority, that authority must inform them of certain matters, some of which are explained further below:

- the role of the prescribed authority;
- the period for which the warrant is in force;
- what the warrant authorises ASIO to do, the person's obligations under the warrant, and the limited right against self-incrimination;
- whether the warrant authorises their detention and if so, for how long;
- whether there is any limit on the person contacting others and, if the warrant permits the person to contact identified persons at specified times when the person is in custody or detention authorised by the warrant, who the identified persons are and what the specified times are;
- the person's right to complain to the Inspector-General of Intelligence and Security about the conduct of ASIO;
- the person's right to complain to the Ombudsman about the conduct of the AFP;
- the person's right to complain to the relevant State complaints agency about the conduct of State police;
- the person's right to seek a remedy from a federal court.

This last piece of information must be reiterated at least once in every 24-hour period during which questioning occurs.

On the first occasion that a person is present during the questioning, the prescribed authority must also explain the reason why that person is present.

Rights to make contact with others (and to make complaints)

Sections 34F, 34G, 34K, 34ZF and 34ZG, ASIO Act

A person taken into custody and detained (whether pursuant to a questioning and detention warrant or on direction of the prescribed authority or because s/he did not appear before a prescribed authority when s/he was obliged to) may not contact anyone, and may be prevented from contacting anyone, while in custody or detention.

There are some exceptions to this. As noted above, a warrant must permit a person to contact a lawyer. A questioning and detention warrant may also identify other people whom the person is allowed to contact, such as a family member or guardian.

The prescribed authority may also direct that a person be permitted to contact a particular individual (who may be identified by their family or legal relationship to the person), though s/he may specify that certain information not be disclosed during the contact.

Finally, the person is permitted to contact the Inspector-General of Intelligence and Security (to complain about ASIO's conduct), the Commonwealth Ombudsman (to complain about the AFP's conduct), or State complaints agency (to complain about the conduct of State police). Facilities must be provided to allow an oral or written complaint to be lodged and it is an offence for those detaining the person knowingly to fail to provide facilities for a complaint (maximum penalty: 2 years' imprisonment). The right to make complaints includes the right to make complaints about breaches of the Protocol.

The role of the Inspector-General of Intelligence and Security

Inspector-General of Intelligence and Security Act 1986; Sections 34P, 34Q, 34R, 34ZI and 34ZJ, ASIO Act

The Inspector-General of Intelligence and Security Act 1986 gives the Inspector-General of Intelligence and Security ('the Inspector-General') the power to take complaints, either orally or in writing, about ASIO. A person in custody must be given facilities to send a sealed envelope with a written complaint to the Inspector-General. That person is also entitled to receive a reply in a sealed envelope.

The Inspector-General must also be kept informed of the process of issuing and taking action pursuant to a warrant. In particular, the Director-General must, as soon as practicable, give the Inspector-General:

- a copy of the draft request seeking the Attorney-General's consent to a request for a warrant;
- a copy of any warrant issued;
- a copy of video recordings made; and
- a statement detailing seizures, custody and detention.

The Inspector-General must also be kept informed of the process of issuing and taking action pursuant to a warrant.

The Inspector-General (or a member of his/her staff) may be present at the questioning or arrest of a person pursuant to a warrant.

If a person has previously been detained pursuant to a warrant and a questioning and detention warrant is issued in relation to him/her, the Inspector-General must inspect the Director-General's draft request, to determine whether or not it contained the relevant additional information required for such a later warrant.

The Inspector-General has no power to stop the execution of a warrant. If, however, s/he is concerned about illegality or impropriety, s/he may communicate this to the prescribed authority (and if s/he does so, s/he must also communicate the concern to the Director-

General as soon as practicable afterwards). The prescribed authority must consider the Inspector-General's concern, and may give directions deferring the exercise of authority under the warrant, or other directions s/he believes necessary, until satisfied that the Inspector-General's concern has been satisfactorily addressed. Such breaks in questioning do not count against the maximum time for questioning.

Federal Court Remedies

Decisions made under the ASIO Act are exempted from judicial review pursuant to the *Administrative Decisions (Judicial Review) Act 1977* (see section 3(d) for definition of 'decision to which this act applies', Schedule 1).

There is, however, the possibility of seeking administrative law remedies pursuant to section 75(v) of the Constitution. Such remedies must be sought in the Federal Court or the High Court. The ASIO Act does not permit a detained person to contact the court directly. In practice such contact would depend on the person instructing a lawyer.

Right to an interpreter

Sections 34M, 34N and 34ZF, ASIO Act

An interpreter may be requested by the prescribed authority if s/he believes on reasonable grounds that the person being questioned cannot communicate with reasonable fluency in English. An interpreter may also be requested by the person being questioned, but this request may be refused if the prescribed authority believes on reasonable grounds that the person being questioned can communicate with reasonable fluency in English. Once the prescribed authority has decided that an interpreter will be present, questioning must be deferred until the interpreter is present, and it is an offence to begin questioning before then (maximum penalty: 2 years' imprisonment).

Limited protection against self-incrimination

Section 34L, ASIO Act

The person being questioned under a warrant does not have a right to refuse to answer a question or to produce a record or thing simply because it might tend to incriminate them or make them liable for a penalty. The person does have some protection against self-incrimination. Anything said in response to a request made during questioning before a prescribed authority under a warrant is not admissible in criminal proceedings against the person, other than offences against section 34L (e.g. failing to provide information, providing a false statement). This also applies to any record or thing produced.

The person does not have 'derivative use' immunity. This means that information, records or things they provide could potentially be used as a basis on which to obtain other

The person being questioned under a warrant does not have a right to refuse to answer a question or to produce a record or thing simply because it might tend to incriminate them or make them liable for a penalty.

evidence. That other evidence would be admissible in criminal proceedings even though it was derived from the inadmissible evidence.

Involvement of lawyers

Sections 34ZO, 34ZP, 34ZQ and 34ZV, ASIO Act

If the subject of a warrant contacts a lawyer, that lawyer must be given a copy of the warrant by ASIO.

The ASIO Act explicitly permits questioning to take place in the absence of a lawyer. If, however, the prescribed authority wishes to allow questioning only when a lawyer is present, then s/he may use his/her authority to make that direction. If present, the person's lawyer may only intervene in questioning or addressing the prescribed authority to seek clarification of an ambiguous question. The prescribed authority, however, must provide a reasonable opportunity for legal advice to be given during breaks in questioning. In addition, during breaks in questioning the lawyer may seek to address the prescribed authority. If the authority considers that the lawyer's conduct is unduly disrupting the questioning, s/he may direct that the lawyer be removed from the place where the questioning is occurring. If this happens, s/he must allow the person to contact a different lawyer.

When a person detained pursuant to a warrant seeks to contact their lawyer, they may be stopped from doing so by the prescribed authority. This may only occur where the prescribed authority is satisfied that if the person contacts their lawyer:

- a person involved in a terrorism offence may be alerted that the offence is being investigated; OR
- a record or thing that the person may be requested to produce in accordance with the warrant may be destroyed, damaged or altered.

If a person detained pursuant to a warrant contacts a lawyer, then the contact must be made in such a way that ASIO can monitor it.

If this happens, the person may contact a different lawyer but the prescribed authority has the same right to stop that contact.

If a person detained pursuant to a warrant contacts a lawyer, then the contact must be made in such a way that ASIO can monitor it. (This is not the case if a person subject to a questioning warrant is not being detained and contacts a lawyer at a time when they are appearing before a prescribed authority for questioning.)

The ASIO Act explicitly preserves legal professional privilege.

Restrictions on travel that flow from seeking, or issuing, a warrant

Sections 34W, 34X, 34Y and 34Z, ASIO Act

Once the Director-General seeks the Attorney-General's consent to a request for a warrant in relation to a person, as soon as practicable after that person is notified of the Director-

General's action, s/he must deliver all his/her passports, Australian and foreign, to a police or customs officer (maximum penalty for failure to do so: 5 years' imprisonment). Once the person is notified of the Director-General's action, it becomes an offence for him/her to leave Australia without the Director-General's written permission (maximum penalty: 5 years' imprisonment).

The ASIO Act does not specify a time limit within which the Attorney-General must refuse or agree to the Director-General's request. Consequently, these provisions seem to give ASIO a reasonably open-ended power to curtail people's overseas travel rights, by seeking permission to request warrants in respect of them.

Likewise, once a warrant has been issued in relation to a person, as soon as practicable after that person is notified of the issue of the warrant, s/he must deliver all his/her passports, Australian and foreign, to ASIO (maximum penalty for failure to do so: 5 years' imprisonment). Once the person is notified of the issue of the warrant, it becomes an offence for him/her to leave Australia without the Director-General's written permission (maximum penalty: 5 years' imprisonment).

Passports must be returned to a person and overseas travel becomes legal:

- if the Attorney-General does not consent; OR
- the issuing authority refuses the request; OR
- if the warrant is issued, once it ceases to be in force.

For the obligations and offences in relation to passports and travel to be enlivened, a person must have the effect of the relevant statutory provision explained to them.

Special provisions relating to children

Sections 34ZC, 34ZE and 34ZR, ASIO Act

Children under 16

A person under the age of 16 years cannot be the subject of one of these warrants.

Children between 16 and 18: issuing of warrants

The Attorney-General may only consent to a warrant in relation to a person between 16 and 18 years old if s/he is satisfied on reasonable grounds that it is likely that the person has committed, is committing or will commit a terrorism offence.

In addition, if the Attorney-General and/or the issuing authority believes on reasonable grounds that the person named is between 16 and 18 years old, then s/he may consent to the request for and issue of the warrant only if satisfied on reasonable grounds:

- that the warrant authorise questioning before the prescribed authority only in the presence of a parent or guardian of the person or, if that is not acceptable to the young person, of another appropriate person (that is, a person who is able to represent the young person's interests, as far as practicable in the circumstances acceptable to

A person under the age of 16 years cannot be the subject of one of these warrants.

the person and to the prescribed authority; and who is not a police officer or an ASIO officer or operative);

- that the warrant authorise questioning before the prescribed authority only for continuous blocks of 2 hours or less, separated by breaks directed by the prescribed authority;
- in the case of a questioning and detention warrant, that the warrant permit the young person to contact a parent, guardian or other appropriate person at any time when the young person is in custody or detention.

Children between 16 and 18: process of questioning

When a young person is brought before a prescribed authority for questioning, if the prescribed authority is satisfied on reasonable grounds that the person named is at least 16 but not yet 18, then as soon as practicable s/he must do the following things:

- inform the person that s/he may request that one parent, guardian or one other appropriate person be present during questioning;
- inform the person that s/he may contact a parent, guardian or other appropriate person at any time s/he is in custody or detention, and direct that such contact be permitted;
- inform the person that s/he may contact a single lawyer of his/her choice while in detention;
- if the person requests the presence of a parent or guardian during questioning, direct that no questioning is to take place in the absence of the parent or guardian;
- if the person does not request the presence of a parent or guardian during questioning, direct that no questioning is to take place in the absence of another appropriate person;
- direct that questioning is to take place only for continuous blocks of 2 hours or less, separated by breaks directed by the prescribed authority.

If a prescribed authority considers that the conduct of a parent, guardian or other representative's conduct is unduly disrupting questioning, s/he may direct that the person be removed from the place of questioning. If this happens, the prescribed authority must:

- inform the person that s/he may request a different parent, guardian or other appropriate person to be present during questioning, and that s/he may contact that person to make the request, and direct that such contact is to be permitted;
- if the person requests the presence of their parent or guardian, direct that no questioning is to take place in the absence of the parent or guardian;
- if the person does not request the presence of their parent or guardian during questioning, direct that no questioning is to take place in the absence of another appropriate person.

Children between 16 and 18: strip searches

If in the opinion of the prescribed authority a person is at least 16 but under 18, or is incapable of managing his/her affairs, then that person may be strip-searched only if the prescribed authority orders that the search be conducted (that is, consent is not sufficient). A strip search must be conducted in the presence of a parent or guardian of the person, or, if that is not acceptable to the person, another appropriate person.

Secrecy provisions and access to information

Section 34ZS, ASIO Act

While a warrant is in force, it is an offence to disclose information:

- indicating the fact that the warrant has been issued;
- indicating a fact relating to the warrant's content;
- indicating a fact relating to the questioning or detention of a person in connection with the warrant (maximum penalty: 5 years' imprisonment).

While a warrant is in force, and for 2 years following its expiration, it is an offence to disclose operational information acquired as a direct or indirect result of the warrant.

While a warrant is in force, and for 2 years following its expiration, it is an offence to disclose operational information acquired as a direct or indirect result of:

- the issuing of the warrant;
- the doing of anything authorised by the warrant;
- the doing of anything authorised by a direction given by the prescribed authority in connection with the warrant;
- the doing of anything authorised by Division 3, Part III in connection with the warrant (maximum penalty: 5 years' imprisonment).

'Operational information' means:

- information that ASIO has or had;
- a source of information (other than the person specified in the warrant) that ASIO has or had; or
- an operational capability, method or plan of ASIO.

This is likely to include information relating to someone's treatment pursuant to the warrant.

Depending on exactly what it means to acquire information as an 'indirect result' of the issuing of a warrant, this may also include information relating to ASIO's follow-up activities in relation to a warrant.

These offences may be committed wherever in the world the disclosure takes place. It is also no defence that the information was acquired as a result of someone else's disclosure.

Strict liability as to the nature of the information applies if the accused is the person in relation to whom the warrant was issued, or his/her lawyer (who was either present at questioning or who provided advice and/or representation in relation to the warrant). In any other situation, at a minimum, recklessness is required.

Permitted disclosures

Certain disclosures are permitted and do not constitute offences against the secrecy provisions.

There are limited exemptions for disclosures connected to complaints and legal proceedings. A disclosure is permitted if:

- it occurs in the course of making a complaint to the Inspector-General of Intelligence and Security, to the Commonwealth Ombudsman, or to a State police complaints agency; OR
- it is made to a lawyer in order to obtain legal advice in connection with a warrant; OR
- it is made to a lawyer in order to obtain representation in legal proceedings seeking a remedy relating to a warrant or the treatment of a person in connection with a warrant; OR
- it is for the purpose of the initiation, conduct or conclusion (by judgment or settlement) of legal proceedings relating to such a remedy.
- There are also wide-ranging exemptions for official disclosures:
- Regulations may be made prescribing certain disclosures.
- The Director-General and (after obtaining advice from the Director-General) the Attorney-General may give written permission for a disclosure.
- A disclosure occurs pursuant to carrying out a direction from a prescribed authority, or is permitted to be made by the prescribed authority. Note that the prescribed authority may give written permission to a lawyer to disclose information to a specified person.
- Disclosures are permitted if they result from a person doing their duty under the ASIO Act, or under a warrant authorised by that Act, or during questioning under a warrant.
- A disclosure is permitted if it results from the exercise of a legislative duty in relation to complaints against the AFP, ASIO or State police.

In deciding whether or not to permit a disclosure by a person, the Director-General, the Attorney-General or the prescribed authority must have regard to the person's family and employment interests (to the extent that they are aware of them), to the public interest, and to the risk to security if permission is given.

As noted, the ASIO Act explicitly preserves legal professional privilege. This may protect certain evidence about disclosure from being led against a defendant. Other types of privilege that may be relevant include parliamentary privilege (for example, information provided to parliamentary inquiries may be unable to be led as evidence in some circumstances).

...the ASIO Act explicitly preserves legal professional privilege.

One important class of disclosure is not expressly permitted. That is, disclosures for the purpose of investigating and prosecuting the various offences the ASIO Act creates in relation to breaches of safeguards (i.e. pursuant to section 34ZF). This seems to significantly lessen the effectiveness of those provisions.

Permitted disclosures where a parent, guardian or other appropriate person is involved

The parent, guardian or other appropriate person may make certain disclosures of otherwise protected information without committing an offence:

- to a parent, guardian or sibling of the person, or to another appropriate person contacted by the person being questioned or present during the questioning of that person;
- to a prescribed authority or other person;
- to a person exercising authority under the warrant;
- to the Inspector-General of Intelligence and Security, to the Commonwealth Ombudsman or to a State police complaints agency.

The prescribed authority may also give written permission to such a representative to disclose information to the specified person.

Complaints about ASIO

Complaints about the conduct of ASIO officers or the organisation more generally should be made to the Inspector-General of Intelligence and Security. These complaints may be made either orally or in writing. Generally, it is a good idea to prepare a statement detailing the experiences of the complainant. It should be clear from the complaint which conduct is the subject of concern. It may be useful to refer to the ASIO Act and the Attorney-General's Guidelines (see above), if these have been breached by ASIO in some way.

The Inspector-General will consider the matters raised in the complaint and will decide whether to investigate the complaint. S/he will then advise the complainant or his/her representative as to whether the complaint is going to be investigated. S/he will also keep the complainant informed about the progress of the investigations.

The Inspector-General has wide-ranging powers of investigation and reporting in relation to ASIO, and may recommend that someone receive compensation if they have been adversely affected by ASIO's actions. Where s/he believes ASIO has not responded appropriately to the recommendations of a report, s/he may raise the matter with the Attorney-General and the Prime Minister.

Complaints about the conduct of ASIO officers... should be made to the Inspector-General of Intelligence and Security.



AFP POWERS

The *Crimes Act 1914 (Cth)* ('the Commonwealth Crimes Act') gives AFP members broad powers to search and question.

In addition, pursuant to the *Australian Federal Police Act 1979 (Cth)* ('the AFP Act'), AFP officers may stop and search a person in a range of listed circumstances, such as where there is a reasonable belief that the person has something s/he will use to cause damage or harm to a place or person 'in circumstances that would be likely to involve the commission of a protective services offence' (section 14J).

Furthermore, AFP officers are permitted to demand a person's name and proof of identification where there are reasonable grounds to believe that the person might have just committed, might be committing or might be about to commit a protective service offence (section 14J).

The definition of a 'protective service offence' encompasses the various terrorism offences that exist under the Criminal Code (section 4).

Investigation Periods

Sections 23CA–23E, *Crimes Act 1914 (Cth)*

The Commonwealth Crimes Act provides at section 23CA that where a person is arrested for a terrorism offence, that person may be detained in order to investigate whether that person has committed that or another terrorism offence. In this context, 'investigating' means questioning the person.

While the 'investigation period' is generally a 'reasonable time' with a maximum of 4 hours, the Act allows for repeated extension of the 'investigation period' up to a total of 20 hours (i.e. a total of 24 hours). The investigation period referred to here is effectively a period in which the police may question the person. That means that the police may question a person for a total period of 24 hours under these powers.

A judicial officer may extend the 4-hour questioning period if satisfied that:

- the offence is a terrorism offence;
- further detention of the person is necessary to preserve or obtain evidence or to complete the investigation into the offence or into another terrorism offence;
- the investigation into the offence is being conducted properly and without delay; and
- the person, or his/her lawyer, has been given the opportunity to make representations about the application.

While the questioning period can be extended any number of times, as noted above, the total time period of questioning cannot exceed 24 hours.

Furthermore, section 23CA of the Commonwealth Crimes Act provides for a range of events that will be disregarded for the purposes of calculating the investigation period, that is, 'dead time' periods. These include (among other things):

- any time used to transport the person;
- any time during which questioning is suspended or delayed while the subject is contacting friends or relatives;
- any time during which questioning is suspended to allow a friend, relative or lawyer to arrive;
- any time during which questioning is suspended or delayed for medical treatment of the subject;
- any time questioning is suspended or delayed because the subject is intoxicated; and
- any time questioning is suspended or delayed to allow the person to rest and recuperate.

There is also a 'catch-all' provision that allows any 'reasonable time' (i.e. a time during which questioning of the person is reasonably suspended or delayed) to be disregarded as 'dead time'. For this time to be disregarded, the approval of a judicial officer (magistrate, bail justice or justice of the peace) is required. For this kind of suspension, the police must provide the judicial officer with a statement that includes the reasons why the police believe the time should be disregarded. These reasons may include:

- the need to collate and analyse information relevant to the investigation (from sources other than the person being questioned);
- the need to allow authorities in or outside Australia time to collect information relevant to the investigation on the request of the police;
- the fact that the police have requested the collection of relevant information from a place outside Australia that is in a different time zone;
- the fact that translation is necessary to allow the police to seek information from a place outside Australia and/or be provided with such information in a language that the police can understand.

If the police make such an application, the person involved or his/her lawyer may make representations to the judicial officer about the application.

In determining the application, the judicial officer may specify a further period of 'dead time' only where it is satisfied that:

- it is appropriate to do so considering the application, the representations of the person or his/her lawyer, and any other relevant matters;
- the offence is a terrorism offence;
- the detention of the person is necessary to preserve or obtain evidence or to complete the investigation into the offence or another terrorism offence;

- the investigation into the offence is being conducted properly and without delay; and
- the person, or his/her lawyer, has been given the opportunity to make representations about the application.

Given all of the periods that may be disregarded as detailed above, a person may be detained by the AFP for a significant period for the purposes of investigation before being charged or released without charge.

At the time of publication, this power had been used once only in July 2007. After terrorist activity in England and Scotland in which a number of suspects were arrested, Doctor Mohammed Haneef (who was related to one of the suspects) was detained in Queensland. In this case, Dr Haneef was detained for a total of 12 days. After an initial 12 hours of questioning, the police repeatedly sought extension of the 'dead time' for the purposes of collating and analysing information. Contrary to the legislation, it appears that on the first extension Dr Haneef was not legally represented. Then, on two occasions, the proceedings relating to the police's subsequent applications to extend were adjourned. In these circumstances, the 'dead time' period extended to any time reasonably required to make and dispose of an application for an extension (see section 23CA(8)(h)). These adjournments therefore resulted in further periods of detention for Dr Haneef.

All proceedings in relation to this matter were conducted in closed court and the identity of the presiding magistrate was suppressed throughout. Furthermore, the grounds and documents relied on by the police in seeking repeat extensions were not made available to the Dr Haneef's lawyer.

Eventually Dr Haneef was charged with recklessly providing support to a terrorist organisation, but this charge was ultimately withdrawn.

Power to Obtain Documents

Section 3ZQN, Commonwealth Crimes Act

This section gives the AFP the power to obtain documents relating to serious terrorism offences, which include all the offences under the Criminal Code discussed above, except for the association offence.

This power arises where an authorised AFP officer considers on reasonable grounds that a person has documents (including in electronic format) that are relevant to, and will assist in, the investigation of a serious terrorism offence. The authorised AFP officer may then apply to a federal magistrate for a notice requiring that person to produce the relevant documents.

The federal magistrate may only grant such a notice where s/he is satisfied on the balance of probabilities that:

- the person has documents that are relevant to, and will assist in, the investigation of a serious offence; AND
- giving the person a notice under this section is reasonably necessary and reasonably appropriate, and adapted to the purpose of investigating the offence.

The notice may only require the person to produce documents that are in his/her possession and that relate to determining one or more of the following matters laid out in section 3ZQP of the Commonwealth Crimes Act:

- whether an account is held by a specified person with a specified financial institution and details relating to the account and/or related accounts;
- whether a specified person is a signatory to an account with a specified financial institution and details relating to the account and/or related accounts;
- whether a transaction has been conducted by a specified financial institution on behalf of a specified person and details relating to the transaction (including details relating to other parties to the transaction);
- whether a specified person travelled or will travel between specified dates, or specified locations and details relating to the travel (including details relating to other persons travelling with the specified person);
- whether assets have been transferred to or from a specified person between specified dates and details relating to the transfers (including details relating to the names of any other person to or from which the assets were transferred);
- whether an account is held by a specified person with a specified utility (such as gas, water or electricity) and details relating to the account (including the names of any other person who also holds the account);
- who holds an account with a specified utility (such as gas, water or electricity) at a specified place, and details relating to the account;
- whether a telephone account is held by a specified person, and details relating to the account including:
 - details of calls made to or from the relevant telephone number;
 - the times at which calls were made or received;
 - the lengths of such calls;
 - the telephone numbers to which such calls were made and from which such calls were received;
- who holds a specified telephone account, and details relating to the account;
- whether a specified person resides at a specified place;
- who resides at a specified place.

The notice must specify:

- the name of the person it is given to;
- the matters to which the documents to be produced relate;
- the manner in which the documents are to be produced;
- the place at which the documents are to be produced;
- that the person must comply with the notice as soon as practicable;
- the effect of failing to comply
- the effect of disclosing the existence or nature of the notice (if the notice specifies that information about the notice must not be disclosed).

Under section 3ZQS it is an offence to fail to comply with a notice to produce documents (maximum penalty: 30 penalty units).

Under section 3ZQT it is an offence for a person who has been given such a notice to disclose the existence or nature of the notice where the notice specifies that information about the notice must not be disclosed (maximum penalty: 120 penalty units or 2 years' imprisonment, or both). It is important to note that this offence does not apply where the disclosure is made for certain purposes, such as:

- to obtain a document from another person (where that other person is directed not to inform the person to whom the document relates about the notice); OR
- to obtain legal advice or representation; OR
- in the course of legal proceedings.

...it is an offence to fail to comply with a notice to produce documents.



SPECIAL POLICE POWERS

Under Commonwealth and State anti-terrorism legislation, the AFP and State police have been given special powers to stop, search and question people.

Commonwealth Legislation

Sections 3UA–3UK, Division 3A, *Crimes Act 1914* (Cth) (Crimes Act)

The Crimes Act has been amended to give all police officers powers to stop, question and search people with respect to 'terrorist acts'.

First, these powers are invoked in relation to people who are present in a 'Commonwealth place'. A 'Commonwealth place' is one where the Commonwealth has the power to make laws, such as defence property or Parliament House. In order to exercise the powers with respect to a person in such a place, a police officer must suspect on reasonable grounds that the person might have just committed, might be committing or might be about to commit a terrorist act.

The powers may also be exercised *carte blanche* in a 'prescribed security zone' (explained below). That is, in a prescribed security zone no reasonable suspicion regarding the commission of a terrorist act is required.

Where the above circumstances apply, police will have the power to ask a person for his/her name, address and proof of identity. Police may also require the person to explain why they are in that particular place. Police will further have the power to stop and detain a person for the purpose of conducting a search for a terrorism-related item, as well as powers to seize items found.

...the Government may declare a prescribed security zone where they believe that such a declaration will assist in preventing a terrorist act or in responding to a terrorist act that has occurred.

Prescribed Security Zones

Broadly, the Government may declare a prescribed security zone where they believe that such a declaration will assist in preventing a terrorist act or in responding to a terrorist act that has occurred.

A declaration may apply to a particular zone for up to 28 days.

As soon as a declaration has been made in relation to a particular zone, police have the power to stop, search and question any person found within that zone during the period specified in the declaration. This power applies to both State police and AFP officers operating within a Commonwealth prescribed security zone

Victorian Legislation

Sections 21A–21X, Part 3A, *Terrorism (Community Protection) Act 2003* (Vic) ('the Terrorism (Community Protection) Act')

Generally, Victorian police are able to stop and demand the name and address of a person where it is reasonably suspected that the person is committing or has just committed a criminal offence or may have knowledge or evidence of the commission of an indictable offence.

In 2006 Victorian counter-terrorism legislation was amended to provide all police officers, State and AFP, with special extended powers, once authorisation for those powers has been given.

To obtain authorisation for the special police powers, the Chief Commissioner of police must apply to the Supreme Court. In emergencies the Chief Commissioner can give an interim authorisation that lasts for a maximum of 24 hours. An authorisation ordered by the Supreme Court generally lasts a maximum of 14 days.

The Supreme Court may make an order authorising the use of the special police powers in the following circumstances:

- where there is an event involving a large number of attendees or the attendance of a prominent person that might be the subject of a terrorist act and an order relating to the event is necessary to protect those attending the event;
- where a terrorist act is occurring or there is a threat that it will occur in the next 14 days and making an order will substantially assist to prevent the terrorist act or to reduce its impact;
- where a terrorist act has occurred or is occurring and the making of an order will substantially assist police to apprehend those responsible or to investigate the act and preserve evidence or it will assist in the community recovery process.
- where an order is reasonably necessary to protect part of an essential service from a terrorist act or to mitigate the effects of a terrorist act on an essential service or to aid the recovery of an essential service from a terrorist act.

To obtain authorisation for the special police powers, the Chief Commissioner of police must apply to the Supreme Court.

The special police powers that are triggered by the above authorisations include the power to:

- obtain disclosure of identity;
- stop and search any person or anything in their possession;
- search vehicles;
- move vehicles;
- enter and search premises;

- cordon off an area for in order to search persons, vehicles or premises; and
- seize or detain things found during searches.

These powers may be exercised by any police officer, State or AFP, and by any person acting under the instructions of a police officer (although the latter are prevented from conducting strip searches).

Police may also use such force as is reasonably necessary to exercise the above powers.

At the date of this publication, the only authorisation obtained under State legislation so far (to the authors' knowledge) related to the Queen's luncheon at the Commonwealth Games in Melbourne in 2006. As a result of this authorisation, police were lawfully able to search a protester who they did not manage to search in the course of their searches at the entry point to that area. There was no requirement that they suspected that the protester was likely to commit a 'terrorist act' or was in any way connected to terrorist activity. It was sufficient that they were exercising their special power to search that person pursuant to an authorisation.



VICTORIA POLICE

Sections 5–13, Part 2, Terrorism (Community Protection) Act 2003

Under Part 2 of the Terrorism (Community Protection) Act Victoria Police may obtain covert search warrants.

A member of the police force may apply to the Supreme Court for a covert search warrant where that member suspects or believes, on reasonable grounds, any of the following:

- that a terrorist act has been, is being or is likely to be committed; OR
- that a person who resides at or even visits the premises:
 - has done an act in preparation for or planning a terrorist act; or
 - has given training to or received training from a terrorist organisation and that training was connected with preparation for or planning or engaging in or assisting in a terrorist act; OR
- that there has been or is activity on those premises connected with preparation for, planning, engaging in or assisting a terrorist act; AND
- the entry and search of the premises would substantially assist in preventing a terrorist act (including by gaining knowledge of an act being done in preparation for, or planning, a terrorist act or connected with the engagement of a person in, or assistance in, a terrorist act or suspected terrorist act); AND
- it is necessary for the entry and search to be conducted without the knowledge of any occupier of those premises.

*Under Part 2 of
the Terrorism
(Community
Protection) Act
Victoria Police
may obtain covert
search warrants.*

The police member's suspicion or belief does not have to relate to a specific terrorist act.

The police member must get the approval of the Chief Commissioner, a Deputy Commissioner or an Assistant Commissioner before making an application for a covert search warrant.

An application for a covert search warrant will be heard in closed court.

When making the application, the police member must provide a supporting affidavit setting out the grounds on which the warrant is sought. In addition, the Court may also require the police member to provide further information concerning the warrant, either orally or in writing. All information provided by the police member must be verified before the court on oath or affirmation or by affidavit.

The Supreme Court may issue a warrant if it is satisfied that there are reasonable grounds for the suspicion or belief founding the application.

In making a decision, the Court must have regard to:

- the nature and gravity of the terrorist act or suspected terrorist act;
- the extent to which the exercise of powers under the warrant would assist the prevention of, or response to, the terrorist act or suspected terrorist act;
- the extent to which the privacy of any person is likely to be affected; and
- any conditions to which the warrant may be made subject.

A warrant must specify all of the following:

- that the purpose of the warrant is to assist the prevention of or response to a terrorist act, or suspected terrorist act;
- the address or location of any premises to which the warrant relates;
- the name of the applicant;
- the name or a description of any other person who may enter premises named or described in the warrant;
- whether more than one entry of the premises named or described in the warrant is authorised;
- the date on which the warrant was issued;
- the period during which the warrant is in force (being a period of no more than 30 days);
- the names of the occupiers of the premises specified in the warrant (if known);
- if relevant, the name or a description of the kind of thing to be searched for, seized, placed, copied, photographed, recorded, operated, printed, tested or sampled; and
- if applicable, any further conditions to which the warrant is subject.

The issue of more than one covert search warrant in respect of premises is possible.

A covert search warrant authorises the police to:

- enter (by force or impersonation if necessary) any premises named or described in the warrant, or other specified premises adjoining or giving access to the premises to be searched;
- search the premises for the kind of thing named or described in the warrant;
- if the warrant authorises seizure of a kind of thing, to seize anything of that kind;
- leave something in place of something seized, if the warrant authorises such a substitution;
- make copies, photograph or record a description of something if the warrant authorises it;

The issue of more than one covert search warrant in respect of premises is possible.

- operate any electronic equipment that is on the premises and copy, print or otherwise record information from that equipment; and
- test or take or keep a sample of something, if the warrant authorises it.

The Terrorism (Community Protection) Act provides that such a warrant may be issued by telephone in urgent circumstances.

Once the police have been granted a warrant, they must report to the Supreme Court within 7 days after the warrant expires. The report must:

- state which powers were exercised under the warrant;
- give details of the compliance with the conditions, if any, to which the warrant was subject;
- state the period during which the entry and search was conducted;
- state the name or description of any person who entered the premises referred to in the warrant;
- state the names of the occupiers of the premises (if known);
- give details of the seizure, placement, copying, photographing, recording, operation, printing, testing or sampling of anything; and
- give details of the benefit derived from executing the warrant for the prevention of or response to a terrorist act or suspected terrorist act.

This report must not be published unless ordered by the Supreme Court.

Each year the Chief Commissioner of Police must submit a report to the State Attorney-General reporting on the police's use of the covert search warrant regime.

Each year the Chief Commissioner of Police must submit a report to the State Attorney-General reporting on the police's use of the covert search warrant regime.



CONTROL ORDERS

Sections 104.1–104.32, Part 5.3, Schedule 1, Criminal Code

Control orders place restrictions on an individual's behaviour, movements, and so on with the aim of preventing a terrorist act.

Before obtaining a control order, the AFP must first get the Attorney-General's consent, after which the AFP may request that the Federal Court make an interim control order.

To make an interim control order, the Court must be satisfied on the balance of probabilities:

- that the order would substantially assist in preventing a terrorist act; OR
- that the person has given training to or received training from one of the listed terrorist organisations.

The Court must also be satisfied that each of the conditions of the proposed control order is 'reasonably necessary'.

An interim control order is made in the absence of the subject. The interim control order must specify a date on which the subject can attend court for the court to:

- confirm (with or without variation) the interim control order; OR
- declare the interim control order to be void; OR
- revoke the interim control order.

An interim control order must also provide a summary of the grounds on which the order has been made.

An interim control order does not come into force until it has been personally served on the subject. It must be served as soon as practicable after it was made and at least 48 hours before the court date specified in the order.

A confirmed control order can last for a maximum of 12 months.

Control orders may be made in relation to people aged between 16 and 18 years old, but such orders may only last for a maximum of 3 months.

A control order may include conditions that:

- stop the person going to certain places;
- stop the person leaving Australia;
- require the person to remain at specified premises during specified times or on specified days;
- require the person to wear a tracking device;

The Court must also be satisfied that each of the conditions of the proposed control order is 'reasonably necessary'.

- stop the person communicating or associating with certain people;
- stop the person using certain types of technology or telecommunications, for example the internet, email;
- stop the person possessing or using certain articles or substances, for example a telephone, certain chemicals;
- stop the person carrying out certain activities including the person's job;
- require the person to report to police as specified;
- require the person to allow him/herself to be photographed;
- require the person to provide his/her fingerprints;
- require the person to participate in counselling or education.

After a confirmed order has been made, the subject may apply to the court for a revocation or variation of that order.

While a control order is in force, the AFP Commissioner may apply to the issuing court to vary the order by adding to or varying its conditions.

It is an offence to contravene a control order (maximum penalty: 5 years' imprisonment).

At the date of this publication two control orders have been sought. The control order in respect of Jack Thomas was sought on the basis that the subject had trained with the terrorist organisation Al Qa'ida in 2001. Broadly, the grounds for the order stated the following:

- that the defendant admitted that he trained with Al Qa'ida in 2001;
- that as a result of that training, the subject is now an available resource that could be tapped into to commit terrorist acts on behalf of Al Qa'ida or related terrorist cells;
- that the subject is susceptible to others' views and beliefs and has links with extremists who may expose and exploit him;
- that the subject's training with Al Qa'ida may make him an attractive target for 'aspirant extremists' who would seek out his skills and experience to assist them.
- that without the control order the subject could be a resource for the planning or preparation of a terrorist act.

The conditions contained in the interim control order included:

- a curfew;
- reporting conditions;
- fingerprint provision;
- a prohibition on leaving Australia;
- a prohibition on an array of activities relating to explosives and weapons, including acquisition, possession, producing, accessing, etc;
- prohibition on contacting certain individuals, including members of listed terrorist organisations;
- a prohibition on accessing a mobile phone service, telephone service card or landline service that have not been approved by the AFP;
- a prohibition on using public telephones and satellite telephone services; and
- a prohibition on using or possessing firearms.

This interim control order was the subject of an unsuccessful High Court challenge on the basis of unconstitutionality. The High Court found that the law used to impose the interim control order was not unconstitutional in a 5–2 decision.

After approximately 12 months a final control order was not sought by authorities on the basis that the subject entered into an undertaking with somewhat different conditions.

A control order was also sought and obtained in relation to David Hicks. Hicks had been held for a lengthy period by the United States of America government at Guantanamo Bay, Cuba. After a military commission hearing in which he pleaded guilty to 'providing material support for terrorism' he was transferred to an Australian prison. Shortly prior to his release from prison, in December 2007 a 12 month interim control order was sought and obtained in relation to Hicks. The interim order was made on the grounds that Hicks had received training from Al-Qaeda and Lashkar-e-Tayyiba and was at risk of participating in a terrorist act. The interim control order included conditions that Hicks report to the police three times a week, that he reside in South Australia and that he stick to a curfew. The interim control order was confirmed in February 2008, after Hicks' release from prison. At that time the conditions were varied, for example, the reporting condition was reduced to twice-weekly and the curfew was also reduced.



PREVENTATIVE DETENTION

Preventative detention orders are provided for by both Commonwealth and State counter-terrorism legislation.

Commonwealth Legislation

Sections 105.1–105.53, Part 5.3, Schedule 1, Criminal Code

Under the Commonwealth legislation the AFP may apply for a preventative detention order in relation to a person in two sets of circumstances:

- where it is believed that the person:
 - will engage in a terrorist act; or
 - possesses a thing connected with the preparation for or engagement of a person in a terrorist act; or
 - has done something in preparation for or planning of a terrorist act.

The terrorist act referred to here must be imminent and must be expected to occur at some time in the next 14 days AND making the order must be reasonably necessary to prevent a terrorist act occurring.

OR

- where a terrorist act has occurred in the last 28 days and detaining the person is necessary to preserve evidence of or relating to a recent terrorist act.

An initial preventative detention order may be made by a senior AFP officer. An AFP member may then apply to an issuing authority for a continued preventative detention order. A continued preventative detention order may last for a maximum of 48 hours.

Certain judges, federal magistrates, Administrative Appeals Tribunal members and retired judges are issuing authorities for continued preventative detention orders.

The AFP may also apply for a 'prohibited contact order' in relation to a person to prevent that person's communication with a specified other person.

In order to enforce a preventative detention order, police have the power to enter premises. Police also have the power to search the subject of the preventative detention order.

The police are not permitted to question a person while they are subject to a preventative detention order. In addition, the police are generally not permitted to take any identification material such as fingerprints or handwriting from the subject unless the person consents or taking the material is necessary to confirm that the person actually is the subject of the preventative detention order. If identification material is taken from a person, it can only be used to confirm that the person is the subject of the preventative

In order to enforce a preventative detention order, police have the power to enter premises. Police also have the power to search the subject of the preventative detention order.

detention order and it must not be used for any other purpose. The legislation does make provision, however, for a person subject to preventative detention to be given into AFP custody for arrest and questioning under the Commonwealth Crimes Act, or into ASIO custody for questioning pursuant to the ASIO Act.

As soon as practicable after a person is first taken into custody, the police must explain the effect of the initial preventative detention order to the person. The person detained must also be informed of any extension to the preventative detention order.

It is also a legislative requirement that the police treat a detainee 'with humanity and with respect for human dignity' and that the person is not 'subjected to cruel, inhuman or degrading treatment'.

A preventative detention order may be made in relation to persons aged between 16 and 18 years old but not in relation to persons under 16. Special provisions apply to the detention of minors.

Contacting Other People

Generally speaking, a person who is subject to a preventative detention order is not permitted to contact other people. The subject can contact:

- one family member; AND
- one person the subject lives with (if the subject does not live with family members); AND
- his or her employer (if the subject is employed); AND
- one of the subject's employees (if the subject employs people in a business); AND
- one other person with whom the subject engages in business (if the subject engages in business with another); AND
- another person if the police agree to it.

When making this contact the subject can only let the person contacted know that the subject is safe but is not able to be contacted for the time being. The subject cannot disclose that a preventative detention order has been made, the fact that he or she has been detained, or how long the detention will last.

A person being detained is entitled to contact the Commonwealth Ombudsman. The person may also contact a lawyer to obtain advice and representation in relation to the preventative detention order.

The subject cannot disclose that a preventative detention order has been made, the fact that he or she has been detained, or how long the detention will last.

There are special conditions relating to the contact that minors may have with other people subject to a preventative detention order. For example, minors may contact both parents/guardians, they may disclose that they are subject to a preventative detention order and they may have in-person contact with another person for at least 2 hours each day.

Any contact that the subject of a preventative detention order has with another person may be monitored by the police.

Disclosure Offences

As noted above, it is an offence for the subject to disclose:

- that the preventative detention order has been made in relation to him/her; OR
- that the s/he is being detained; OR
- the period of time for which s/he is being detained.

It is an offence for a subject's lawyer to disclose information relating to the preventative detention order, the detention, or any information provided by the detainee to another person except for a purpose related to the preventative detention order.

It is an offence for a subject's lawyer to disclose information relating to the preventative detention order... except for a purpose related to the preventative detention order.

Where the subject is a minor, it is also an offence for the subject's parent/guardian to disclose any information relating to the preventative detention order or the detention.

If the subject improperly discloses information to one of the people the subject contacts, it would be an offence for the recipient of that information to pass it on to anyone else.

These offences are all punishable by a maximum of 5 years' imprisonment.

State Legislation

Sections 13A–13ZV, Part 2A, Terrorism (Community Protection) Act

Each State and Territory has a preventative detention order regime complementary to that established under the Criminal Code, which permits detention on the same grounds for a period of up to 14 days (inclusive of any preventative detention by the Commonwealth or by another State or Territory).

The procedures under these State and Territory regimes correspond broadly to those under the Criminal Code, although some require the police to apply to the Supreme Court for an order, and give the subject of the order a wider range of rights.

In Victoria, the preventative detention regime is established under Part 2A of the Terrorism (Community Protection) Act. It requires an application to be made by an authorised officer of Victoria Police to the Supreme Court of Victoria (see section 13C). In the event that the application is made ex parte, the Supreme Court may elect to issue a merely interim order with a maximum duration of 48 hours or until the matter is reheard for a final determination (sections 13E and 13G). Prohibited contact orders also may be granted only by the Supreme Court, in a hearing at which the subject of the order is entitled to appear (sections 13L and 13M). The civil standard of proof applies in cases relating to preventative detention orders (section 13ZO).

Under the Victorian regime, a detainee may apply to the Supreme Court for revocation or variation of a preventative detention or prohibited contact order. The Court may not grant leave for such an application unless satisfied that new facts or circumstances have arisen (section 13N).

Under the Victorian legislation, when contacting a family member or other person whom s/he is permitted to contact, the subject of a preventative detention order is permitted to disclose that s/he is subject to a preventative detention order. S/he is also permitted to disclose the period for which s/he is being detained. The order may also specify additional rights of contact (including visits) with family members or other persons (section 13ZD).



NATIONAL SECURITY INFORMATION LEGISLATION

National Security Information (Criminal and Civil Proceedings) Act 2004 ('NSI Act')

The NSI Act is generally aimed at preventing disclosure of information in federal criminal proceedings and civil proceedings where the disclosure is likely to be prejudicial to national security. The exception to this is that disclosure must be allowed to the extent that preventing the disclosure would seriously interfere with the administration of justice.

The NSI Act requires legal representatives in federal criminal proceedings to obtain security clearances before they can access security-sensitive information. In civil proceedings, parties or their legal representatives may also be required to obtain a security clearance where there may be disclosure of information related to national security.

The NSI Act provides for the management of sensitive information in federal criminal proceedings, including the following:

- Before a trial begins, the defendant or prosecutor can ask the court to arrange a pre-trial conference in which matters relating to national security information can be discussed.
- Prosecutors and defendants are required to notify the Attorney-General if they believe that they, or a witness they are calling, will:
 - disclose information relating to national security, or
 - disclose information where disclosure in the criminal proceedings may affect national security.
- The Attorney-General then has the power to order the person not to disclose the information except in 'permitted circumstances'.

In civil proceedings, the NSI Act provides that:

- Before the substantive hearing a party to the proceeding may ask the court to hold a conference in which the parties can consider matters relating to disclosure of security-sensitive information.
- Parties are required to notify the Attorney-General about potential disclosures of security-sensitive information in the same way as in federal criminal proceedings (as described above).
- The Attorney-General then has the power to order the person not to disclose the information except in 'permitted circumstances'.

The NSI Act requires legal representatives in federal criminal proceedings to obtain security clearances before they can access security-sensitive information.

Generally, 'permitted circumstances' refers to disclosure in the course of a person's duties in relation to the proceedings.

The Attorney-General's Department has also issued 'Requirements for the Protection of National Security Information in Federal Criminal Proceedings and Civil Proceedings'. These requirements give practical guidance on how national security information is to be stored, handled, accessed, destroyed, returned after proceedings and so on. The requirements relating to information vary depending on whether the information is classified as 'Top Secret', 'Secret', 'Confidential' or 'Restricted'.

The NSI Act creates a number of offences for making prohibited disclosures and for otherwise failing to comply with the requirements created by the NSI Act.



SEDITION

Sections 80.2–80.6, Division 80, Criminal Code

In late 2005, amendments were made to Division 80 of the Criminal Code in relation to sedition offences, despite much protest against the changes. Under section 80.2 the offence of 'sedition' now includes:

...the Attorney-General's written consent is required before the commencement of proceedings on sedition offences.

- urging another person to overthrow the government or constitution by force or violence. This offence can be committed recklessly, that is, where the person committing the offence is reckless that it is the government that they are urging the other person to overthrow.
- urging another person to interfere by force or violence in processes for a parliamentary election. Again, this offence can be committed recklessly.
- urging a group, or groups, to use force or violence against another group where that use of force would threaten the peace, order and good government of the Commonwealth. This offence can also be committed recklessly.
- urging a person to assist an organisation or country that is at war with Australia, that is, to assist an enemy. There is a defence to this offence where the urging relates to the provision of humanitarian aid.
- urging another person to assist an organisation or country that is engaged in armed hostilities against the Australian Defence Force. Again, there is a defence where the urging relates to the provision of humanitarian aid.

It is important to note that the Attorney-General's written consent is required before the commencement of proceedings on sedition offences.

Extended geographical jurisdiction applies to sedition offences. This means that the offences encompass seditious conduct that occurs outside Australia.

Exceptions

Section 80.3 provides for a number of exceptions to the sedition offences. Broadly stated, these are the exceptions:

- trying in good faith to show that the Sovereign, the Governor-General or a state Governor, inter alia, are mistaken in their counsels, policies, or actions;
- pointing out, in good faith, governmental errors or defects, with a view to reforming those errors or defects (this includes State, Federal and foreign governments);
- urging someone to lawfully procure social change;
- pointing out in good faith any matters that are producing or may produce feelings of ill will or hostility between groups in order to resolve those issues;

- doing anything, in good faith, in connection with an industrial dispute;
- publishing, in good faith, a report or commentary about a matter of public interest.

The onus is on the defendant to bring evidence to show that they fall within the scope of an exception. Once enough evidence has been adduced to discharge this burden, the onus is on the prosecution to demonstrate that the exception does not apply.



MORE INFORMATION AND RESOURCES

- 'ASIO, The Police and You' booklet produced by Australian Muslim Civil Rights Advocacy Network (AMCRAN) <<http://amcran.org>> (The third edition of this booklet is going to be published shortly and will be available in English, Arabic, Bahasa Indonesia and Urdu.)
- Federation of Community Legal Centres <<http://www.communitylaw.org.au>>
- Activist Rights Website <<http://www.activistrights.org.au>>
- Australian Parliament Website <<http://www.aph.gov.au>>
 - Follow the library link to 'criminal law' and then to the specific material about terrorism. There are lots of links on policy, the law and international matters
- Australian National Security <<http://www.nationalsecurity.gov.au>>
 - Includes access to all anti-terrorism legislation
- Commonwealth Attorney General's Department Website <<http://www.ag.gov.au>>
 - Follow the link on the homepage to 'National security and counter-terrorism'
- For further legal advice:
 - Western Suburbs Legal Service, (03) 9391 2244
 - Federation of Community Legal Centres, (03) 9654 2204
 - Victoria Legal Aid, (03) 9269 0234
 - Law Institute Referral Service, (03) 9607 9355 (for referral to a private solicitor)

NOTES

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

[illegible]

The Federation of Community Legal Centres (Vic) Inc

Suite 11, First Floor

54 Victoria Street

Carlton South VIC 3053

Email: administration@fclc.org.au

Website: www.communitylaw.org.au



Federation of
Community Legal Centres
VICTORIA

