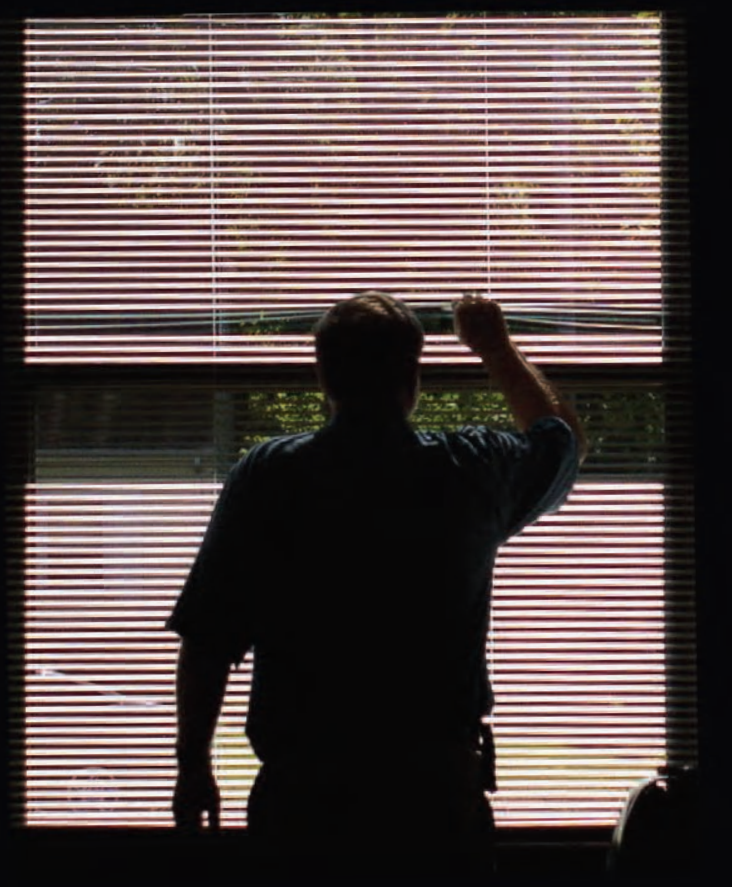

What Price Security?

Taking Stock of Australia's Anti-Terror Laws

Andrew Lynch & George Williams

WHAT PRICE SECURITY?

TAKING STOCK OF AUSTRALIA'S ANTI-TERROR LAWS

Andrew Lynch is the Director of the Terrorism and Law Project at the Gilbert + Tobin Centre of Public Law and a Senior Lecturer in the Faculty of Law, University of New South Wales.

George Williams is the Anthony Mason Professor and Director of the Gilbert + Tobin Centre of Public Law at the Faculty of Law, University of New South Wales.

BRIEFINGS

A series of topical books exploring social, political
and cultural issues in contemporary Australia

Series editors: Peter Browne and Julian Thomas
Australian Policy Online (www.apo.org.au)
Institute for Social Research, Swinburne University of Technology

What Price Security?

Taking Stock of Australia's Anti-Terror Laws

ANDREW LYNCH
& GEORGE WILLIAMS

UNSW PRESS

A UNSW Press book

Published by
University of New South Wales Press Ltd
University of New South Wales
Sydney NSW 2052
AUSTRALIA
www.unswpress.com.au

National Library of Australia
Cataloguing-in-Publication entry

Lynch, Andrew, 1973– .

What price security?: taking stock of Australia's anti-terror laws.

ISBN 9780868409092.

ISBN 0 86840 909 X.

1. Terrorism – Law and legislation – Australia. 2. Terrorism – Prevention – Government policy – Australia. 3. Terrorism investigation – Australia. 4. Civil rights – Australia. I. Williams, George, 1969–. II. Title.

345.9402

Cover photograph: Robert Kyllo/iStockphoto.com

Printed by Hyde Park Press

Australian Government
Australian Research Council

This project has been assisted by the Australian Government through the Australian Research Council

Contents

Preface

The aim of this book is to provide readers with a straightforward guide to the major counterterrorism laws passed by the Australian parliament in the five years since the attacks of 11 September 2001. The need for strong terrorism laws is often the subject of heated public debate, but it is difficult to follow and participate in these discussions without an understanding of what laws we already have and how they work.

Parts of this book are developed from earlier writings, including submissions made to parliamentary and other committees about the new laws. Some were prepared with our colleagues Dr Ben Saul and David Hume, and we acknowledge their influence on this work. We thank Edwina MacDonald and Tessa Meyrick for their assistance in writing this book and Dominique Dalla Pozza for her comments on a draft of the manuscript.

Andrew Lynch and George Williams

Introduction

We live in what is often referred to as the post-9/11 world. Terrorism has become the defining concept of our time. Indeed, the indications are that the threat has not subsided in the wake of the attacks on 11 September 2001, but may have increased. The mastermind of the 9/11 attacks, Osama Bin Laden, remains at large, and there have been major attacks on civilians since in Bali, Madrid, London and Mumbai. Even when we are not directly touched by such atrocities, we often fear the possibility of terrorist violence.

We can also be affected personally by the responses of governments in areas like airline security. In August 2006 it appeared that British authorities had foiled a plot to explode a number of planes en route to the United States, but the threat still led to chaos at airports around Britain as strict controls on passengers and their carry-on baggage were introduced.

Terrorism is not only a problem overseas. Twenty-eight people have been arrested and charged under the new terrorist offences in Australia. One Australian was accused, though ultimately acquitted, of plotting to enter government buildings to shoot their occupants. Another, Faheem Lodhi, was sentenced to twenty years in jail for making preparations that could have led to the bombing of defence force bases and the Sydney electricity grid. Jack Thomas was convicted for receiving funds from a terrorist organ-

isation while in Pakistan; although his conviction was quashed on the grounds that his key admissions were not voluntary, he then became the subject of the first control order made under Australian anti-terror legislation. Meanwhile, two groups of men await trial: a group in Melbourne is accused of being members of a terrorist organisation planning training activities and a group in Sydney is charged with conspiring to prepare a terrorist attack.

Events like these are happening now. But while Australia should hold fast and adopt measures to prevent harm to innocent people, confronting terrorism is not as straightforward as it might appear. Our response to terrorism raises vitally important questions of law and policy. How can we best defend ourselves from terrorists? Should the Australian Security Intelligence Organisation, ASIO, have the power to detain citizens for questioning? Is it appropriate to place people under house arrest without finding them guilty of an offence? Do we need safeguards to ensure that evidence obtained by torture is not used in terrorism trials? Should governments be able to access our emails and text messages without our knowledge? Is there, ultimately, a right way to fight the "war on terror"?

These and similar questions have been the subject of such spirited public debate in Australia that it seems incredible that only five years ago we had no national laws addressing terrorism. To the extent the threat was discussed, we were content for the ordinary criminal law to deal with terrorism and other forms of political violence.

Unlike other countries, Australia has had a fortunate existence almost entirely free of acts of political violence over the course of the twentieth century. Perhaps the most well-known act of terrorism in Australia was the bombing of the Sydney Hilton Hotel during the Commonwealth Heads of Government Regional Meeting in 1978. There have been other acts of political violence, such as the bombing campaign against justices of the Family Court in the early 1980s, but on the whole the threat of terrorism was rarely considered.

To have continued in our relaxed attitude to the threat of terrorism after September 11 would have amounted to complacency or even naivety. The development of a specific and coordinated policy for national security had clearly become a priority. In pursuit of this goal, over the last five years the Commonwealth has made 37 new laws that directly deal with counterterrorism – an average of one new law every seven weeks. In September 2006 five more laws were before parliament.

The purpose of this book is to provide an accessible guide to the major components of Australia's anti-terrorism laws. National security is inevitably a complex topic, but the Australian public has also had to contend with the sheer volume of law-making. There has been so much law over such a short time – much of it amending and broadening what was passed just months earlier – as to render the overall impact impenetrable for the interested citizen.

In this book we unpack Australia's new terror laws to give readers a clear idea of the main issues. We look at what amounts to a crime of terrorism in Australia, what powers ASIO has to question and detain members of the community, and what happens when the authorities seek a control order or an order of preventative detention over an individual. We look at what kinds of speech risk making a person liable for the crime of sedition, and we show how judicial processes have been modified for the trial of people charged with terrorism offences.

We are mainly concerned with Commonwealth laws. Although the states and territories have not been idle in legislating for security, with some choosing to enhance police powers significantly, they have played a supporting role to the national government. They have even transferred some of their constitutional powers to the Commonwealth for its use.

Because it is important not to consider these laws in a vacuum, we compare the Australian legislation to laws introduced overseas and assess their relative impacts on basic freedoms. We also look at the lessons of history, including our

own. Crucially, the laws should not be seen as applying only to "someone else" – they affect the whole Australian community, whether directly or indirectly.

•

At the outset, we need to recognise that there is clearly some level of threat to Australia. Dennis Richardson, the former Director-General of ASIO, has revealed that "al-Qaida had an active interest in carrying out a terrorist attack in Australia well before 11 September and… we remain a target."[1] The present Director-General, Paul O'Sullivan, has confirmed that "ASIO currently assesses a terrorist attack in Australia as feasible and [it] could well occur."[2] These concerns are reflected in the government's 2004 white paper, *Transnational Terrorism: The Threat to Australia*.

Statements like these need to be assessed in light of the information the government makes publicly available on its national security website, <www.nationalsecurity.gov.au>, which was created to inform Australians of the threats and what is being done to deal with them. The site contains a four-level alert system (low, medium, high and extreme) that currently rates Australia as being at a medium level of alert. Until 2005 the system unhelpfully defined a "medium" level of alert to be a "medium risk of a terrorist attack in Australia"; this was changed so that the medium alert means (still unhelpfully) that a "terrorist attack could occur." The alert level has remained at medium since September 2001.

Making a sufficient response to this uncertain threat involves creating offences that recognise the seriousness of the crime of terrorism and granting our intelligence and law-enforcement agencies the powers they need to protect us. But this must not be the only approach if we are to win the "war on terror." We also have to ensure that we preserve our way of life – and particularly the basic freedoms and access to justice that are consistent with our position as one of the world's oldest continuous democracies.

These dual objectives do not produce an impasse, but a need for balance. Rights are not absolute, but they can guide us when we are working out just how far the law should sensibly go. Strong counterterrorism laws are justified where it can be shown that they will help to meet the threat and that they have been drafted in such a way as to have as little impact as possible on fundamental freedoms. It is vital that governments and parliaments around the world recognise the need for justification and proportion in responding to national security threats.

This approach is not "soft on terror." On the contrary, it has solid legal and historical credentials. Even at the onset of the second world war the government recognised that wartime controls must not undermine Australia's identity as a free and democratic society. Introducing national security legislation in September 1939, the Prime Minister, Robert Menzies, told parliament:

> Whatever may be the extent of the power that may be taken to govern, to direct and to control by regulation, there must be as little interference with individual rights as is consistent with concerted national effort… [T]he greatest tragedy that could overcome a country would be for it to fight a successful war in defence of liberty and to lose its own liberty in the process.[3]

His words are just as apt today.

Menzies's own government forgot this insight during the late 1940s and early 1950s as Australia grappled with the external and internal dangers posed by communism. With community fears fed by political and media hysteria over an unseen enemy, federal parliament enacted dramatic legislation. Anyone who knowingly carried or displayed any material indicating that he or she was in any way associated with the Communist Party faced five years in jail. The legislation gave the government the power to ban organisations and to declare people to be "communists" merely on its assessment of their beliefs.

Despite fundamental differences between that time and ours, a few parallels are too striking to be denied. Today, as then, the enemy is seen as an ideology or belief rather than a foreign power. Although there are geographic frontlines in the conflict – not Korea and Vietnam this time, but Afghanistan and Iraq – the "war" is not merely "over there" but something that may strike us at home. And yes, the anti-terrorism laws of today strongly echo Menzies's flawed Communist Party Dissolution Bill.

Fortunately, the High Court struck down that law, and in the subsequent referendum the majority of the electorate denied parliament the power to re-enact it.[4] Despite this reversal for the government, Australia was kept safe from the threat of communism. As these events show, even when they act with the best of intentions governments sometimes adopt measures that can result in an unacceptable loss of liberties – as Menzies himself had recognised in 1939. Today, it is vital that in fighting the "war on terror" we do not allow ourselves to become the victims of our own fears.

CHAPTER 1

Crimes of terror

Responding to the events of 11 September 2001, Australia created a series of new criminal offences – Divisions 101, 102 and 103 of Part 5.3 of the Criminal Code – covering conduct related to committing and planning terrorist acts.[5] The first two Divisions distinguish between offences committed by individuals acting alone and offences where criminal liability depends on some connection to a terrorist organisation. Division 103 creates offences relating to financing terrorism. Each of these federal criminal offences needs to be understood in conjunction with the general principles of criminal responsibility – including fault and the level of proof – set out in Chapter 2 of the Criminal Code.

Some have argued that these new offences were not needed. After all, laws covering murder, violence and the destruction of property are among the oldest we have, and could be used to prosecute terrorists. But this approach has not been favoured by countries with a history of terrorism, many of which felt the need for new laws after 9/11. Terrorism has features that distinguish it from other crimes – not least of which is the scale of harm it seeks to inflict. Motivation is also important, for in seeking to instil "terror" in the populace the terrorist is often indiscriminate in his or her target. Terrorism is thus a crime committed against the entire community. Special criminal offences are an appropriate response to terrorism's unique characteristics.

WHAT IS A TERRORIST ACT?

Section 100.1 of the Criminal Code defines a "terrorist act" to be an action – or threat of action – done with the intention of:

- "advancing a political, religious or ideological cause"; and
- "coercing, or influencing by intimidation" an Australian or foreign government or "intimidating the public."

The second requirement was not in the original Bill introduced into parliament after September 11. It was added on the unanimous recommendation of the Senate Legal and Constitutional Committee after an outcry from legal and community groups. Without it, the definition did not clearly focus on the intent associated with terrorist acts, which distinguishes them from other activities also motivated by a political, religious or ideological cause, which may incidentally cause harm to others.

The "action" that is committed or threatened may take a number of forms:

- causing physical harm to or death of a person;
- causing serious damage to property;
- endangering the lives of others;
- creating a serious risk to the health or safety of the public; or
- seriously interfering with electronic systems of finance, communications, services and transport. (This reflects the modern possibilities of cyber-terrorism whereby damage is done or threatened without itself directly causing loss of life.)

The Code is careful to establish what does *not* amount to terrorist action. This is important because the law needs to distinguish legitimate activities – political protest or industrial action, for example – from terrorism. This aspect of the law also underwent major modification as it progressed through parliament. Initially the draft section simply provided an exception for "industrial action and *lawful* advocacy, protest or dissent" (empha-

sis added). This had the potential to sweep into the classification of "terrorism" many forms of civil protest (unlawful perhaps only owing to trespass or a failure to obey police instructions) in which people, property or electronic systems are harmed or damaged.

Under the law as finally passed, *any* "advocacy, protest, dissent or industrial action" will not be regarded as a terrorist act, so long as it is not carried out with the intention of, for example, causing a person's death or risking the safety of the public. But the government remains unhappy about this exception. In early 2006 the Security Legislation Review Committee, which was appointed under the *Security Legislation Amendment (Terrorism) Act 2002* and included independent members such as the Commonwealth Ombudsman, conducted a thorough review of terrorism offences and took submissions from interested parties and the public. The Attorney-General's Department proposed dropping the part of the definition of "terrorist act" that protects ordinary forms of protest. Although the committee did not accept that suggestion, the government may well propose the change again in the future.

An example demonstrates why the qualifications in the definition are vital. If parents of schoolchildren organised a rally in a public park without permission in order to protest about the state of public education, this could have fallen within the scope of "terrorism" under the original version of the section. The activity was clearly designed to advance a political cause (the funding of education) with a view to influencing government policy, and might not have been "lawful" because the organisers had failed to obtain a permit. If prosecutors could also show that the event posed a serious risk of danger to the public (by virtue, say, of congregating a large, unmanageable crowd near other users of the park and adjoining roadways) then that might have been sufficient to make the rally breach the law as originally drafted.

It is highly unlikely that the organisers of such an event would be prosecuted for terrorism. But that is not the point. The law should not be so loosely drafted that activities like these could so easily slip within the meaning of "terrorism" and thus attract

severe penalties for the individuals involved. In seeking to counter terrorism, governments must be careful not to stifle legitimate dissent. Clearly, advocacy that seeks to influence public and political opinion falls well short of intimidation. But such questions may often be a matter of degree, and the express protection of acts of protest and dissent is vital to ensuring a limited scope for the Code's terrorism provisions.

The Australian definition is more carefully drafted than those adopted in the United Kingdom and the United States, for example, which do not exclude advocacy, protest and industrial action. But it is not free of complications. It does not, for instance, clarify whether the actions of a nation as part of an armed conflict can amount to terrorism (the definition would seem to include them). Further problems stem from the fact that the term "terrorism" is so contested – as are the political uses to which it is put, such as in the 2006 conflict in Israel and Lebanon. What some see as terrorism, others see as defence or a struggle for liberation. After all, Nobel Peace Prize winner Nelson Mandela was called a terrorist by many people – including British Prime Minister Margaret Thatcher – during his fight against apartheid in South Africa. He would also be classified as a terrorist under Australian law, for the law applies to terrorism both in and outside of Australia and makes no allowances for someone who causes harm as part of a struggle for liberation.

DIVISION 101 – OFFENCES BY INDIVIDUALS

The core offence in Division 101 is that of engaging in a terrorist act (section 101.1). Because the definition of a terrorist act includes a threat to commit such an act, a person may be charged with this crime even though no attack has occurred. Anyone found guilty is liable to a maximum punishment of life imprisonment. No one has been charged with this offence to date.

The other crimes in Division 101 are "ancillary offences": they do not deal with terrorist acts but actions that are connected to them. It is an offence if a person intentionally:

- "provides or receives training" (section 101.2);
- "possesses a thing" (section 101.4); or
- "collects or makes a document" (section 101.5)

that is "connected with preparation for, the engagement of a person in, or assistance in a terrorist act."

These offences are committed if the person either knows or is reckless as to the fact (that is, aware of a substantial risk) that they relate to a terrorist act. The maximum penalty for each offence varies between ten and 25 years' imprisonment, with the higher penalties applying where actual knowledge can be proved. While there is no doubt that terrorism is a very serious crime, these penalties are extremely high. It is not easy to see why possessing things or documents which might never be used can attract a greater punishment than do crimes such as rape or people-trafficking.

Under section 101.6, it is also an offence intentionally to do "any act in preparation for, or planning, a terrorist act." A person found guilty is liable to life in jail. Like the offences relating to training and the commission of a terrorist act, this section applies to the activities of people anywhere in the world. Since 2005, all these offences are committed under the Code even if:

- a terrorist act does not occur;
- the training/thing/document/other act is not connected to a specific terrorist act; or
- the training/thing/document/other act is connected to more than one terrorist act.

The scope of these ancillary offences are a source of concern. In criminalising the very formative stages of an act, they render individuals liable to very serious penalties despite the lack of a clear criminal intent. This is a significant extension of traditional concepts of criminal responsibility since it is far removed from the commission of an unlawful act. The law has long recognised

offences based on an attempt to commit a crime, or even a conspiracy to do so. But the ancillary offences in Division 101 establish crimes at an even earlier point.

In parliament, the Minister for Justice and Customs, Senator Chris Ellison, offered this justification for the offences:

> In the security environment that we are dealing with, you may well have a situation where a number of people are doing things but you do not yet have the information which would lead you to identify a particular act… When you are dealing with security, you have to keep an eye on prevention of the act itself as well as bringing those who are guilty of the act to justice.[6]

This comment reveals a policy of using the law not merely to punish or deter specific conduct but to prevent such conduct. Authorities are now empowered to act pre-emptively by arresting people before they have formed a definite plan to commit the criminal act – an approach that reflects the growing dominance in counterterrorism law of what is known as the "precautionary principle." While stopping a terrorist act from taking place must be our aim, there are constraints on the extent to which the criminal law may be used to achieve this without compromising its integrity. This is particularly the case when the hooks on which offences hang are not tightly circumscribed. Terms such as "training," "thing," "document" and "any act" are not defined in the Criminal Code and their meanings are far from precise. Moreover, the offences (particularly those relating to possession and collection) are drafted in such a way that authorities have a wide discretion over whether to lay charges and prosecute in each case. It is conceivable that people who are simply foolish or careless might find themselves being prosecuted.

Section 101.5, for example, criminalises the act of collecting or producing a document that is "connected with preparation for, the engagement of a person in, or assistance in a terrorist act." The defendant must have known or been reckless as to the

connection, but the offence is committed even if the document is not connected to a *specific* terrorist act. The effect of such open-ended drafting is to expose to liability a person who, for example, downloads from the internet a document providing instructions on bomb construction. Because there is a substantial risk that others may be using that information to plan some sort of terrorist activity, the first person will be liable – even though his or her reason for obtaining the document may be entirely innocent, such as academic or media research or curiosity.

This lack of discrimination arises because section 101.5 fails to draw a necessary connection between the person who collects the document and the document's use in the preparation of a terrorist act. The defendant must know, or be reckless as to the fact, that the document is connected with preparation for a terrorist act. But what is missing from the crime is a requirement that he or she collects the document *with the intention* of using it to assist in preparation of a terrorist act. Instead, this crucial consideration arises later in the section, as a defence on which the defendant can rely if he or she can show that, in collecting the document, he or she did not intend to facilitate or assist in the doing of a terrorist act. The evidential burden is placed on the defendant: he or she has to point to evidence to show that there is a reasonable possibility that he or she had no such intention before the prosecution will be called on to establish such an intention. Certainly, the prosecution must refute the defence's claims beyond a reasonable doubt, but the defendant effectively has to argue his or her innocence first. This is a significant departure from the accepted notion in Australian criminal law that the prosecutor should be required to prove all the central elements of an offence before a person has to mount a defence.

Shifting the evidential burden onto the defendant is particularly worrying because of the breadth with which these offences are expressed. Doubtless these provisions were designed to deal with people who are stockpiling chemicals or documenting strategically important sites. But the laws do not provide others

with sufficient certainty about what could expose them to prosecution. This problem is compounded by the lack of any requirement for the prosecution to show that the preparatory activity or thing or document was connected to a particular terrorist plot. That sets a very low bar for authorities who have great discretion as to when to lay charges.

If those concerns seem alarmist, there remains a very practical argument against the width of these offences. Quite simply, they may prove unpredictable in application. The few trials of people charged under these laws (see chapter 5) suggest that the looseness of the offences is difficult to square with the requirement that the jury be satisfied of guilt "beyond reasonable doubt." The provisions may well enable charges to be laid on the strength of conduct that is not obviously connected to a specific terrorist act, but this does not necessarily mean that juries will feel confident in finding guilt – especially with such serious penalties attached. Having such broad ancillary offences might encourage authorities to act precipitately. It is true that with delay may lie danger, but to arrest people on the basis of activities or possessions that cannot, at that point, be connected to any terrorist act creates the risk that the courts will not be convinced a crime was in fact committed.

DIVISION 102 – TERRORIST ORGANISATIONS

What is a "terrorist organisation"?

Under the Criminal Code, there are two ways that a group can come within the definition of "terrorist organisation." The first is if it is "directly or indirectly engaged in, preparing, planning, assisting in or fostering" a terrorist act (whether or not one occurred as a result). The prosecution must prove not only that these activities took place but also that they were carried out by a discernible group of people working as an organisation. Thus, the first formal recognition of a group as a "terrorist organisation" could come when charges are laid. This risks exposing those who are at the fringes of a group to unexpected and unwarranted liability.

The second and far clearer way in which a group may be a "terrorist organisation" is if it is proscribed (or banned) as such by the federal Attorney-General. By September 2006 nineteen organisations had been banned under Australian law.* While proscription enables people to know which groups they should avoid, it raises concerns. Until 2004 the Australian government could only proscribe organisations that had been identified by the United Nations Security Council. In 2004, parliament passed a law allowing the Attorney-General to proscribe organisations reasonably believed to be involved in terrorist activity; the prior permission of parliament is no longer required. This means that the government now has an independent power to ban organisations. While it would be difficult to challenge in court a decision to proscribe a group, the Criminal Code does provide that a decision can be reviewed by a parliamentary committee and disallowed by parliament. No such disallowance has yet occurred.

In reporting on its review of the laws in June 2006, the Security Legislation Review Committee expressed deep concern over the proscription process. It recommended that either the power be exercised by the Federal Court on application by the Attorney-General or, if the Attorney-General retained the power, that the discretion be guided by an advisory committee comprised of security, legal and public affairs experts. The committee stressed that affected individuals and organisations must be given notice of the intended proscription and the ability to oppose it.

At present, a group may be proscribed by virtue of its activities – essentially, the Attorney-General must be satisfied that the

* The organisations are: Abu Sayyaf Group, Al Qa'ida, Al-Zarqawi, Ansar Al-Islam, Armed Islamic Group, Asbat al-Ansar, Egyptian Islamic Jihad, Hamas's Izz al-Din al-Qassam Brigades, Hizballah External Security Organisation, Islamic Army of Aden, Islamic Movement of Uzbekistan, Jaish-i-Mohammed, Jamiat ul-Ansar (formerly known as Harakat Ul-Mujahideen), Jemaah Islamiyah, Kurdistan Workers Party (or PKK), Lashkar I Jhangvi, Lashkar-e-Tayyiba, Palestinian Islamic Jihad, and the Salafist Group for Call and Combat.

body is directly or indirectly engaged in, or preparing for, terrorist acts – or if the Attorney-General decides that it advocates terrorist activity. Advocacy is defined as directly or indirectly counselling, urging or providing instruction for a terrorist act. It also includes directly praising terrorism in circumstances where there is a risk that this might lead a person to engage in a terrorist act. It is unclear when an organisation can be said to be "praising" terrorism. Must the praise take place publicly or will private statements suffice? Must the organisation as a whole formally praise terrorism, or are the words of a leader (or even a single member) sufficient? If the latter, it is possible that an organisation may be banned on the basis of statements that not all its members support. Once banned, the organisation's members face jail under the "ancillary offences" outlined below.

What might such "praise" look like? An example might be something like the statement by Cherie Blair, wife of the British Prime Minister, who said of the Israeli–Palestinian conflict: "As long as young people feel they have got no hope but to blow themselves up you are never going to make progress."[7] The comment provoked uproar on the basis that it might be seen as excusing, if not justifying, suicide bombing. The Prime Minister's office later issued an apology.

This statement might fall within the definition of "advocacy." In attempting to explain the causes of terrorism, organisations such as Red Cross or Amnesty International must also take care not to be seen as supporting such activities. If they were, then on a strict reading of the Criminal Code the Attorney-General would be entitled to proscribe the organisation and its members could face criminal prosecution.

In reality we would be very surprised to see decisions like this being made. But this does not mean that the law should not worry us. It still has a significant operation in that it "chills" our freedom of speech. Outspokenness is replaced with caution and timidity of expression. This aspect of Australia's counterterrorism regime is discussed further in chapter 4.

Offences relating to "terrorist organisations"

Division 102 creates offences based on a person's relationship with a terrorist organisation. It is an offence if a person intentionally:

- "directs the activities" of a terrorist organisation (section 102.2);
- "is a member" of a terrorist organisation (section 102.3);
- "recruits a person to join, or participate in the activities of," a terrorist organisation (section 102.4);
- "provides training to," or "receives training from," a terrorist organisation (section 102.5);
- "receives funds from, or makes funds available to," a terrorist organisation (section 102.6);
- provides "support or resources" to a terrorist organisation (section 102.7); or
- "associates with another person who is a member of, or a person who promotes or directs the activities of," a terrorist organisation (section 102.8).

Many of these offences apply to situations in which the defendant either actually knew or was reckless as to an organisation's status as a "terrorist organisation." Some, however, only require one of these standards of knowledge.

Like the offences in Division 101, these crimes can be remote from an actual terrorist act. For example, under section 102.5 a person may be guilty of intentionally providing training to or receiving training from a terrorist organisation if he or she is reckless as to its character as such an organisation. But there is nothing in the offence that requires the training *itself* to be connected to a planned terrorist activity. Undoubtedly running camps dedicated to weapons training would be covered by the section, but so might training of any other kind, such as instruction in the use and maintenance of office equipment. As a result,

the offence is not appropriately targeted and exposes people to liability when their activity has no direct connection to terrorism at all. This may be contrasted with the offence of providing "support or resources" to a terrorist organisation in section 102.7, which requires that the support or resources will help the organisation engage in planning a terrorist activity.

The most controversial of the offences found in Division 102 relate not to activity conducted in connection with an organisation but to the criminalisation of membership and association. A person offends under section 102.3 if he or she is intentionally a member of an organisation that is a terrorist organisation, and knows it to be so. While this appears straightforward enough at first glance, it should be remembered that these provisions can apply to groups of individuals who amount to an organisation under the law even though they would not regard themselves as an "organisation." Similarly, the Code defines membership to include "informal" members of an organisation. While this aims to address the practical problems surrounding the secret and unstructured nature of terrorist organisations, it makes the question of when someone has crossed the line rather murky.

Section 102.8 is even less precise. It contains the offence of having an "association" with a member (formal or informal) of a group that has been listed as a terrorist organisation. This offence will have been committed if, on two or more occasions:

- a person "intentionally associates with another person who is a member of, or a person who promotes or directs the activities of, an organisation"; and
- "the person knows that the organisation is a terrorist organisation" (though quite confusingly, a later subsection says that the offence will only apply if the person is reckless as to whether the group is listed as a terrorist organisation) and knows that the person they associate with "is a member of, or a person who promotes or directs the activities of, the organisation"; and

- the nature of the association is that it "provides support" to the terrorist organisation that is intended to "assist the organisation to expand or to continue to exist."

However, an "association" is not an offence under a number of circumstances. The defendant bears an evidential burden of proving the association is excused on grounds that include it having taken place:

- "with a close family member and relates only to a matter that could reasonably be regarded… as a matter of family or domestic concern";
- in "a place being used for public religious worship and takes place in the course of practising a religion";
- "only for the purpose of providing aid of a humanitarian nature"; or
- "only for the purpose of providing legal advice or legal representation in connection with" a set range of matters.

This section is also expressly limited by the guarantee implied from the Australian Constitution that communication about political matters should remain free. But the defendant bears the evidential burden of establishing the extent to which the offence is curtailed by this freedom.

In its report to the Attorney-General, the Security Legislation Review Committee was highly critical of almost every aspect of section 102.8. The central concepts of "associate" and "support" were unclear, particularly in their relationship to each other; the level of knowledge required was confused by the subsection insisting on recklessness; and the failure to specify the boundaries of the offence was unsatisfactory. The committee felt that the focus on "association" was provocative to the Muslim community because it targeted a basic human right rather than focusing on those who provided "support" to terrorist groups – an activity that was already criminalised elsewhere in the Division. The com-

mittee recommended that section 102.8 be repealed. It left open an alternative approach: a more carefully targeted offence aimed at a person who provides support to a member of a terrorist organisation with the intention that the support expands, or helps the continued existence of, the organisation. The Attorney-General's Department has said it does not view these changes favourably and will retain section 102.8 in its present form.

FINANCING OFFENCES

Just two criminal offences are found in Division 103 of the Code, and they are very similar. Section 103.1 is the broader of the two, making it an offence for a person to provide or collect funds "reckless as to whether the funds will be used to facilitate or engage in a terrorist act," but not specifying the other party involved. Section 103.2 is more precise in criminalising the act of making "funds available to" or collecting "funds for, or on behalf of, another person (whether directly or indirectly)" with reckless disregard as to whether that person will use the funds for terrorism.

The need for two provisions dealing with the same issue is far from obvious – especially when supplying funds to or receiving funds from a terrorist organisation is already criminalised under section 102.6 in the preceding Division. The Security Legislation Review Committee concluded that section 103.1 is so broadly expressed that it was "hard to see where section 103.2 adds anything of substance."[8]

It is especially important that these offences be stated with precision. They have the potential to affect people quite distant from terrorist activities who give or raise funds for causes or bodies not fully aware of how the money is going to be spent. Section 103.2 expressly provides that even making funds available indirectly will constitute an offence if the person is reckless as to their possible use in financing terrorist activity. The offence does not require any terrorist act to have eventuated. People who donate to an organisation – perhaps knowing no more than the fact that it advocates animal liberation or national independence – are at risk

of being charged if their money is forwarded on to a militant part of that movement (whether or not its terrorist activities take place far away or even not at all). Moreover, the Division's offences are given an extended geographical jurisdiction, meaning that the offence may be committed by a person providing monies overseas.

This is not to say that there are easy solutions to the very real problem of dealing with those who finance terrorism. Invariably, they aim to elude detection by crossing international borders and using organisational "fronts" to screen the real recipients of funds. The provisions of Division 103 are but one aspect of Australia's attempts to prevent and criminalise this activity. Amendments have also been made to the *Financial Transaction Reports Act 1988* to place additional reporting obligations on the banking and financial sector.

•

Central to all of the essential terrorism crimes under the Criminal Code is the definition of "terrorist act." Although terrorism is a difficult concept to pin down, the legislative definition is sufficiently precise for the new criminal offences and protects legitimate forms of protest and advocacy.

But in this chapter we have shown how the actual offences go beyond terrorist action. The ancillary offences outlined in Division 101 are designed to empower authorities to prevent the fulfilment of a terrorist plot. In so doing there is a real risk that they may define liability too broadly so that otherwise innocent behaviour may lead to a person being charged despite the absence of criminal intent.

The offences relating to terrorist organisations in Division 102 contain similar points of uncertainty, and also criminalise some relationships between individuals. Overarching these problems are the flaws in the process by which a group may be proscribed by the Attorney-General as a terrorist organisation, an issue of great importance given the serious consequences it could have on individuals.

CHAPTER 2

Monitoring, questioning and detaining: ASIO's new powers

The most controversial aspect of the federal government's immediate response to September 11 was its decision to grant extraordinary new powers to the Australian Security Intelligence Organisation. ASIO can now question and detain suspected terrorists and monitor them through electronic and other means to gather intelligence that might prevent an attack. But it can also monitor, question and detain Australian citizens who are *not* suspected of any involvement with terrorism but who might have information of use to the government.

The new power to detain innocent Australians generated considerable opposition and many months of heated public debate. The debate centred on whether it is appropriate to confer this power on a secret intelligence organisation and whether the detention of non-suspects for information-gathering purposes can ever be justified.

ASIO'S EVOLUTION

ASIO is at the frontline of the government's war on terrorism. While it is not a police force, its role in collecting and analysing intelligence can be vital to preventing an attack. In the early decades after its creation in 1949, ASIO's main focus was Soviet espionage and subversion. Today, its role is "to gather information

and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's national security."[9] These dangers include espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defence system and acts of foreign interference.

After September 11, as ASIO focused on the threat posed by terrorism, it grew massively. The organisation's current budget is almost five times what it was five years ago, with the total appropriation increasing from $69 million in 2001–02 to $340.6 million in 2006–07.[10] Staff numbers have increased from 584 at 30 June 2001 to 1070 at 25 May 2006, and are forecast to grow to 1860 by 2010–11.[11]

Existing powers

ASIO obtains some of its information from news sources, statistical databases and the intelligence services of other nations. It also gathers information through intrusive methods of investigation, as set out in the *Australian Security Intelligence Organisation Act 1979*.

On request from ASIO's Director-General, the Attorney-General can issue a warrant allowing the organisation to collect intelligence by entering and searching premises, inspecting, removing and retaining records, frisk searching a person, and accessing and copying data on a computer or other electronic equipment. If the Attorney-General is satisfied that a person is, or is reasonably suspected of being, engaged in activities that would prejudice national security, he or she can also issue a warrant allowing ASIO to tap the person's communications, use a tracking device on the person or inspect the person's mail. The warrants are issued for a limited period (up to six months in most cases).

It is an offence, punishable by up to two years' imprisonment, for ASIO employees to communicate intelligence for non-work purposes. Any person who publishes the identity of an ASIO employee (except the name of the Director-General) without the

consent of the Attorney-General or the Director-General can be jailed for up to one year.

Accountability

From its inception ASIO targeted not only communist sympathisers but also Labor Party members and anti-war protesters, so it is not surprising that the organisation attracted suspicion among Labor figures. Two successive Labor governments instigated royal commissions into Australian intelligence agencies, in 1974 and 1983, leading to greater scrutiny and ministerial influence over ASIO.

Yet there remain few avenues for members of the public to seek information about the organisation. The *Freedom of Information Act 1982* does not extend to intelligence agencies, and a person may never find out that he or she has been the subject of an investigation. Instead, the public depends on the vigilance of those who have access to classified information about ASIO's work, namely the Attorney-General, the Parliamentary Joint Committee on Intelligence and Security (previously called the Parliamentary Joint Committee on ASIO, ASIS and DSD) and the Inspector-General of Intelligence and Security.

The Attorney-General has a supervisory role in issuing ASIO warrants, and also issues guidelines to govern the way ASIO performs its functions. ASIO provides a classified annual report to the government, and the Attorney-General tables an unclassified version in parliament.

The Parliamentary Joint Committee on Intelligence and Security is appointed under the *Intelligence Services Act 2001* to review ASIO's administration and expenditure and consider any matter referred by the Attorney-General or a resolution of either house of parliament. But the Act also lists matters that the committee cannot review, including intelligence-gathering priorities, sources of information and individual complaints. ASIO can even censor committee reports. On one occasion, ASIO insisted on the removal of a sentence from a report despite the committee's

protestation that the censored material did not constitute a national security concern. Although the committee regarded the deletion as a violation of its responsibility to report to parliament on the operations of the ASIO legislation, the deleted sentence was not reinstated.[12]

The Office of the Inspector-General of Intelligence and Security provides independent scrutiny of ASIO. Established under the *Inspector-General of Intelligence and Security Act 1986*, the office's role is to assure the public that ASIO conducts its activities according to the law, behaves with propriety, complies with ministerial guidelines and directives, and takes account of human rights. It has extensive information-gathering powers and can take sworn evidence, enter ASIO premises and require a person to answer questions or produce documents. The office has full access to all ASIO records, can initiate its own inquiries (as well as conduct inquiries referred to it by the government) and can examine public complaints.

ASIO'S NEW POWERS

The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002, one of the Howard government's first responses to September 11, was introduced into federal parliament on 21 March 2002. The Bill permitted ASIO to strip-search and detain without trial adults and even children who were not suspects but who may have had useful information about terrorism. Such detention could be for two-day periods that could be renewed indefinitely.

Detainees could be denied the chance to inform family members or their employer of their detention: "A person who has been taken into custody, or detained, under this Division is not permitted to contact, and may be prevented from contacting, anyone at any time while in custody or detention." Detainees had no right to silence and if they failed to answer any question put by ASIO they could serve up to five years in prison. Yet they were only guaranteed access to legal advice *after* the first 48 hours of

detention. Moreover, while the Bill stated that people "must be treated with humanity and with respect for human dignity," there was no penalty for ASIO officers who subjected detainees to inhumane treatment, or even to torture.

This was one of the most remarkable pieces of legislation ever introduced into the federal parliament. It would not have been out of place in General Pinochet's Chile. Nevertheless, the government defended the Bill strenuously, arguing it was a necessary measure to protect Australia against the threat of terrorism. Things soon became unstuck in the Senate, however, where the majority lay with the Labor opposition and the minor parties.

Two parliamentary committees scrutinised the new powers proposed for ASIO. The Parliamentary Joint Committee on ASIO, ASIS and DSD *unanimously* found that the Bill "would undermine key legal rights and erode the civil liberties that make Australia a leading democracy."[13] The government and Labor members of the Senate Legal and Constitutional Legislation Committee rejected the government's proposal for a detention power and put forward a different model based on a power to question; separate minority reports by the Democrats and the Greens expressed outright opposition to the Bill.

In the face of these reports and strong opposition from legal, community and other groups, the Bill stalled. At one point during a continuous 27-hour debate in the final sitting days before Christmas 2002, the government and the Labor opposition each contended that their opponents would have to wear the blame for any Australian blood that might be spilt by terrorists because of the deadlock.

A new version of the law, styled as the ASIO Bill (No 2), was finally passed on 26 June 2003, fifteen months after the beginning of what had proved to be one of the longest debates in the history of federal parliament. Its final form involved compromise on all sides. Under the law, which amended the *Australian Security Intelligence Organisation Act 1979*, Australians could be questioned for 24 hours while being detained for one week. In

addition, a person could only be held and questioned on the order of a judge, with the questioning to take place before a retired judge. These additional, independent protections blunted some of the main problems with the original Bill. Even in this form, however, the laws gave ASIO unprecedented new powers which could be justified only as a temporary response to the exceptional threat to national security posed by terrorism. This was reflected in the sunset clause added to the law, which meant that it was to lapse after three years unless re-enacted.

This much-debated Bill was by no means the end of the government's legislative ambitions in the area. But whereas that Bill had excited great public debate, the subsequent laws, despite their importance, barely rated a mention in the media and generated little opposition from within or outside parliament. With the next law introduced only five months (or 34 parliamentary sitting days) after the ASIO Bill was passed, its opponents were perhaps reluctant to become embroiled in another protracted debate. That next law, the *ASIO Legislation Amendment Act 2003*, increased the time allowed for the questioning of non-suspects by ASIO from 24 to 48 hours when an interpreter is involved. It also made it an offence to disclose "operational information" about detention under the Act.

Since this legislation was passed, five additional laws have further modified ASIO's counterterrorism powers. Among other things, ASIO can now demand the surrender of a person's passport in certain circumstances, can use search warrants for 90 days (up from 28 days) and postal and delivery service warrants for six months (up from 90 days), and can remove and retain for a reasonable period material found during the execution of a search warrant.

One change made in 2006 to the *Telecommunications (Interception and Access) Act 1979* expands ASIO's power to request a warrant from the Attorney-General to intercept the telecommunications of innocent people where this might, for example, "assist the Organisation in carrying out its function of obtaining intelli-

gence relating to security." This vague standard has the potential to authorise ASIO to collect and read all the communications between an innocent party and anyone with whom he or she communicates, including family, friends, lawyers, doctors and so on.

As the end of their three-year life approached in 2005, ASIO's new powers of questioning and detention came up for review. The Parliamentary Joint Committee on ASIO, ASIS and DSD examined the laws and in November 2005 recommended, among other things, that the Act be amended to clarify the operation of the warrants, guarantee the right to a lawyer, require the availability of facilities to make complaints, and retain the sunset clause with a five-year period for review. The Howard government accepted some of these recommendations but rejected others when it drafted the *ASIO Legislation Amendment Act 2006*, which came into force on 20 June 2006. While the new law retains a sunset clause for the powers, it extends this by a further ten years to 2016.

HOW DO THE QUESTIONING AND DETENTION POWERS WORK?

As enacted and amended, the law allows ASIO to seek two types of warrant: one for questioning and the other for questioning and detention.

A questioning warrant permits ASIO to bring a person for questioning before a "prescribed authority" – such as a retired judge with five or more years' experience on a superior court – appointed by the Attorney-General. To obtain a warrant for questioning, the Director-General of ASIO must seek the Attorney-General's consent. Once the consent is given, the Director-General can ask an "issuing authority" (a federal magistrate or judge appointed by the Attorney-General) to issue the warrant. The Attorney-General and the issuing authority must be 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." It is not necessary that the individual to be subject

to the warrant is suspected of any wrongdoing. The Attorney-General must also be satisfied that "relying on other methods of collecting that intelligence would be ineffective" and that there are written procedures on how to carry out the warrant.

Under the warrant, ASIO can ask the person questions and require him or her to provide records or things. The questions or requested items must be relevant to intelligence that is important in relation to a terrorism offence, and the questioning must be recorded on video. The warrant can be in force for up to 28 days and the questioning can last for up to 24 hours (or up to 48 hours if an interpreter is used) in blocks of up to eight hours each.

A person must not refuse to answer the questions put to him or her, or give answers that are "false or misleading." In either case, the penalty is imprisonment for up to five years. Even if the information is self-incriminating the person must provide it. Although it cannot be used in criminal proceedings against them, that protection is limited. The law does not confer a "derivative use immunity," which would prevent disclosures being used to gather other evidence against the person in future criminal proceedings. Nor does it confer any immunity from civil proceedings, where the evidence could be used in proceedings to deport the individual, for example.

Under a questioning and detention warrant a person can be taken into custody by a police officer and questioned by ASIO. The warrant must allow the person to contact a lawyer, family member or other person at specified times while detained. The procedures for applying for and issuing this warrant are much the same as those for a questioning warrant. In addition, though, the Attorney-General must be satisfied that "if the person is not immediately taken into custody and detained, the person: (i) may alert a person involved in a terrorism offence that the offence is being investigated; or (ii) may not appear before the prescribed authority; or (iii) may destroy, damage or alter a record or thing the person may be requested in accordance with the warrant to produce."

A questioning and detention warrant allows for a person to be held for up to seven days; as with questioning warrants, he or she can be questioned for no more than 24 hours (or 48 hours if an interpreter is used) in eight-hour blocks. The person must then be released. But a fresh warrant can then be issued if the Attorney-General and the issuing authority are satisfied that this is justified by "information that is additional to or materially different from that known to the Director-General" when he or she sought the Attorney-General's consent to the previous warrant request.

Different rules apply for people under eighteen years of age. No warrant can be issued for a person who is younger than sixteen. If a person is between sixteen and eighteen, the Attorney-General can only consent to the warrant if he or she is satisfied that "it is likely that the person will commit, is committing or has committed a terrorism offence". A parent, guardian or other interested person can also be contacted and may be present when the minor is questioned.

Obligations arise even before the Attorney-General gives his or her consent to the Director-General's request for a warrant. Once notified of the consent request and the relevant obligations, a person cannot leave Australia without permission and must surrender his or her passport.

Other obligations and powers arise when either type of warrant is issued. In exercising the warrant a police officer can enter premises if he or she believes on reasonable grounds that the person subject to the warrant is there, and can use necessary and reasonable force to search the premises for that person. A police officer can also use the same force to take a person into and prevent them escaping from custody, detain the person and bring them before a prescribed authority for questioning. If a person is detained, a police officer can carry out a search of the person. The police officer can also carry out a strip-search if he or she suspects on reasonable grounds that "the person has a seizable item on his or her person" and "it is necessary to conduct a

strip search of the person in order to recover that item," and if a prescribed authority approves the search.

Under both types of warrants, the person must be allowed to contact a lawyer of his or her choice. But this entitlement is removed when the prescribed authority is satisfied that, if the person contacts a lawyer, the person may alert someone else involved in a terrorism offence that the offence is being investigated, or a record or thing that the person may be asked to produce will be destroyed, damaged or altered.

A person can talk to their lawyer once he or she is present, but the law says that "The contact must be made in a way that can be monitored by a person exercising authority under the warrant." The lawyer cannot interrupt the questioning or address the prescribed authority except to clarify an ambiguous question. On the other hand, there must be breaks in the questioning that provide a reasonable opportunity for the lawyer to advise the person. The lawyer can also ask to talk to the prescribed authority during the break in questioning, but must get the prescribed authority's permission to do so.

Obligations persist after the expiry of the warrant. With few exceptions, a person cannot tell anyone "operational information" obtained through the exercise of the warrant for two years after the warrant has expired. While the warrant is in force, a person is also not allowed to give anyone information about the warrant, including that it has been issued. Any person giving out such information will be committing an offence punishable by up to five years in jail. This applies to lawyers and family members as well as to the person who was detained and questioned. The implications of this aspect of the law for freedom of speech are examined in chapter 4.

The behaviour of police officers and other people executing a warrant is subject to some scrutiny. ASIO must report to the Attorney-General on the usefulness of activities taken under each warrant, and must provide the Inspector-General of Intelligence and Security with copies of items such as requests for warrants,

issued warrants and interview recordings. The Inspector-General examines ASIO's warrant records on a monthly basis. He or she can also be present during questioning and when a person is taken into custody under a warrant, and can raise concerns with the prescribed authority. If a police officer or person executing a warrant does not observe some of the safeguards included in the legislation – for example, by not immediately bringing a person before the prescribed authority for questioning or by subjecting the person to cruel, inhuman or degrading treatment – he or she is guilty of an offence and liable to two years in jail.

The law also requires the Director-General of ASIO to consult the Inspector-General of Intelligence and Security and the Commissioner of the Australian Federal Police in preparing protocols to cover questioning and detention. Protocols cover such details as the manner of questioning (and the use of force), food and sleep facilities and access to health care.

ASIO has not used its extensive new questioning and detention powers excessively. From the time the ASIO Bill was enacted until November 2005, only fourteen questioning warrants were issued covering thirteen people (one person was the subject of two warrants). The greatest number of hours that a person was questioned was 42 hours and 26 minutes (with an interpreter) and 15 hours and 57 minutes (without an interpreter).[14]

•

In the five years since September 11, ASIO has been given greatly enhanced powers and an enormous increase in budget and personnel. Although there is no evidence that ASIO has misused its powers, there remains a risk that they might be misused (whether by deliberate design or genuine mistake).

It is important to remember that ASIO's detention power is more extensive than the powers granted to similar organisations in the United Kingdom, Canada and the United States. Only Australian law allows for the detention in secret of *non-suspect* citizens by an *intelligence agency*. In the United Kingdom the

police may detain suspected terrorists for 48 hours extendable to a total of 28 days, while in Canada the detention period is 24 hours extendable for a further 48 hours. Under the US legislation "inadmissible aliens" can be detained for renewable six-month periods, as can any non-citizen who is engaged in any activity "that endangers the national security of the United States."[15]

Under the ASIO regime an innocent person not suspected of any crime can potentially be detained for longer than a suspect. Under the amended *Crimes Act 1914*, a person arrested for a terrorism offence may only be detained for the purpose of investigating the offence for four hours (or two hours if the person is under eighteen years old, or is Indigenous). This may be extended for up to twenty hours, giving a maximum period of 24 hours before charges must be laid. (By contrast, the investigation period for serious, non-terrorist federal offences may only be extended for up to eight hours to a maximum of twelve hours.) The law therefore permits ASIO to detain non-suspects for seven times longer than people suspected of terrorism offences.

The possibility that expansive powers might be abused by intelligence agencies is very real. For example, in 2002 American judges found that the FBI and the US Justice Department had supplied "false information" in regard to "more than 75 applications for search warrants and wiretaps" for terrorist suspects.[16] Information had also been improperly shared with prosecutors in charge of criminal cases. If this were to occur in Australia, great damage could be done to public confidence in ASIO and its capacity to protect Australian security. It would be unfortunate if people came to fear the organisation for the powers it can wield both for and against Australians.

CHAPTER 3

Pre-emptive policy: preventative detention and control orders

Preventing a terrorist attack is the core aim of the Commonwealth's national security policy, and the law has a central role to play. As Attorney-General Philip Ruddock has made clear, prevention is not just a matter of a telephone hotline, better policing and tightened transport security: "The law should operate as both a sword and a shield – the means by which offenders are punished but also the mechanism by which crime is prevented."[17]

The criminalisation of preparatory activities and the significant expansion of the powers of intelligence agencies, which we have considered in the preceding chapters, are two of the ways in which the aim of prevention has been reflected in legislation. But the counterterrorism laws examined in this chapter offer an even more striking example of the government's attempt to use the law pre-emptively.

In late 2005, as part of a suite of changes agreed to by the Council of Australian Governments in the wake of the London bombings, Divisions 104 and 105 were added to Part 5.3 of the Criminal Code. They enable control and preventative detention orders to be imposed on a person. While both orders are expressly designed to protect the public from a terrorist act, they differ in an important way. Preventative detention orders are fairly short-term. They are aimed at either preventing an imminent terrorist attack or preserving evidence relating to a terrorist

act that has recently taken place. Control orders, on the other hand, while still ultimately aimed at prevention, are not predicated on there being an imminent risk of terrorist attack. They may last much longer – up to a year, with the possibility of renewal. So far there has been only one control order issued and no preventative detention orders.

These orders illustrate the tension in employing the law as a tool of preventative policy. They challenge the traditional purpose of legal regulation. Under neither order is there a need for a person to have been found guilty of, or even be suspected of committing, a crime. Yet both orders enable significant restrictions on individual liberty. This is more than a breach of the old "innocent until proven guilty" maxim: it positively ignores the notion of guilt altogether.

CONTROL ORDERS

Control orders impose a variety of obligations, prohibitions and restrictions on a person for the purpose of protecting the public from a terrorist act. By order of a court, they allow the Australian Federal Police, the AFP, to monitor and restrict the activities of people who pose a terrorist risk to the community without having to wait to see whether this risk materialises.

The potential scope of a control order ranges from a very minimal intrusion on an individual's freedom to an extreme deprivation of his or her liberty. The order can include prohibitions or restrictions on the individual:

- being at specified areas or places;
- leaving Australia;
- communicating or associating with certain people;
- accessing or using certain forms of telecommunication or technology (including the internet);
- possessing or using certain things or substances; and

- carrying out specific activities (including activities related to the person's work or occupation).

The order can also include the requirement that the person:

- remain at a specified place between certain times each day, or on specified days;
- wear a tracking device;
- report to specified people at specified times and places;
- allow photographs or fingerprints to be taken (for the purpose of ensuring compliance with the order); and

If the person consents, they can also participate in counselling or education.

Unlike preventative detention orders, control orders stop short of imprisoning the subject in a state facility. Nevertheless it is clear that it is possible to detain an individual using an order. If a person must not be at specified places or must remain at specified places at certain times then this may amount to detention. It effectively provides a means by which an individual may be placed under house arrest.

A person who contravenes the terms of a control order commits an offence with a maximum penalty of five years' jail.

How is a control order made?

Attorney-General's consent: Only senior members of the AFP may seek control orders. The first step is to obtain the written consent of the Attorney-General to request an interim order from an issuing court. Before seeking consent, the AFP member must have reasonable grounds for either believing that the order would "substantially assist in preventing a terrorist act" or suspecting that the individual over whom the order is sought has provided training to or received training from a proscribed organisation.

The Attorney-General must be provided with a draft request that supports those grounds, detailing the facts on which they are based and an explanation of why the obligations or restrictions

sought in the order should be imposed. The AFP member must also inform the Attorney-General of any known facts that might go *against* imposing the order. An example might be that a restriction on the individual's movement would prevent him or her from continuing in employment and supporting dependants.

The Criminal Code does not specify any matters the Attorney-General must consider before giving his or her consent. This may be contrasted with the requirements for the making of ASIO questioning and detention warrants. The Attorney-General may require changes to the request before granting consent.

Making an interim control order: Once the Attorney-General has granted consent, the AFP member can request the interim control order from an issuing court (the Federal Court, the Family Court or the Federal Magistrates Court). The court must receive the request in the same form as was presented to the Attorney-General, except for any changes required by the latter, together with a copy of the Attorney-General's consent. Under section 104.4 of the Code, the court can only make the order if it is satisfied of the grounds on which the AFP has made the request. The court must believe, on the balance of probabilities, that:

- "making the order would substantially assist in preventing a terrorist act"; or
- "that the person subject to the order has provided training to, or received training from, a listed terrorist organisation."

The court must also be satisfied that the obligations, prohibitions and restrictions are "reasonably necessary, and reasonably appropriate and adapted, for the purpose of protecting the public from a terrorist act." In determining these matters, the court must take into account the impact of an order on the person's circumstances – including financial and personal matters.

The test of "balance of probabilities" is a civil, not criminal, standard of proof. Given the serious consequences that an order

may have for an individual's freedom, it is debatable whether this lower standard is appropriate. In Senate committee hearings about the new law, members of the government sought to defend the use of the civil standard by likening the control orders to search warrants. While such warrants can involve a significant intrusion on an individual's privacy, control orders may impose far greater constraints. A search warrant is also a step in the process of criminal investigation which may lead to charges being laid against someone; a control order is an end in itself.

If the court issues an interim control order it is of no effect until served personally on its subject. The order must set out a summary of the grounds on which it has been made. Surprisingly, this was not required in the early draft of these laws made public on the internet by the Chief Minister of the Australian Capital Territory, Jon Stanhope, yet it is clearly vital if the individual is to be able to challenge the order. The interim order must also inform the person as to when – as soon as practicable but at least 72 hours after the order is made – he or she may attend a court for it to confirm, revoke or declare void the interim control order.

Confirming the control order: After the interim control order is granted and 48 hours before the nominated hearing date, the AFP member must advise the issuing court whether he or she wishes to seek confirmation of the order. The individual affected must also receive this notification along with the documents given to the Attorney-General in order to obtain consent. This is subject to an important caveat: any information that is likely to prejudice national security or put at risk the operations or safety of police, intelligence agencies or the community is exempt from the obligation.

If the AFP has elected to confirm the order, the court will make a decision after a hearing at which both parties can provide evidence and make submissions. This is a vast improvement on the preliminary draft of the law, which did not grant a person the right to appear to challenge the confirmation of a control order.

The court does not, however, require the attendance of that person to act in relation to the order.

The court may declare the order to be void if satisfied that at the time it was made there were no grounds for making it. This seems strange: in effect the court would be saying that its previous decision was without foundation. Far more likely would be a determination by the court that the order should be revoked because *at the present time* (after hearing the submissions of the individual affected) it is not satisfied that the order will substantially assist in preventing a terrorist act or that the person had participated in training activities with a proscribed organisation. Alternatively, the court might still be satisfied, on the balance of probabilities, about either of those factors but might not believe that the terms of the order sought are reasonably necessary or reasonably appropriate and adapted for protecting the public; in this case it may confirm the order but vary or remove some of its restrictions or obligations. If the court remains satisfied on all counts it can confirm the order, which may then last up to twelve months (or three months if the subject is aged sixteen to eighteen years).

Changing or revoking a confirmed control order

The AFP is free to make further requests for new control orders over a person when an order has expired. The same process applies. During the life of a confirmed control order, the AFP Commissioner may apply to an issuing court to add further obligations, restrictions or prohibitions. Owing perhaps to the seniority of his office, the Commissioner does not need to seek the consent of the Attorney-General before doing so.

Once made, an order may be revoked or varied on the application of either the individual affected or the AFP Commissioner. Clearly, there is little point in the individual making the application unless he or she can point to some altered circumstance. In the alternative, he or she can appeal the confirmation of the original order to a higher court.

PREVENTATIVE DETENTION ORDERS

A preventative detention order, or PDO, enables a person to be taken into custody and detained by the AFP for an initial period of up to 24 hours, with an option to have the order continued for a total period not exceeding 48 hours. This time can then be augmented under corresponding state law. At the Council of Australian Governments meeting in September 2005 the premiers and chief ministers agreed to enact legislation enabling longer periods of detention that, owing to concerns over constitutional constraints, the Commonwealth could not enact for itself. State and territory laws (the amended NSW *Terrorism (Police Powers) Act 2002*, for example) extend the period of detention to a maximum of fourteen days. The Criminal Code empowers state and territory courts to review the making of a PDO and the treatment of the subject under the Commonwealth provisions and to grant the same remedies as they might for breaches of their own jurisdiction's scheme. These courts cannot, however, exercise this jurisdiction while the Commonwealth's order is still in force.

How is a preventative detention order made?

The issuing authority: Under the Criminal Code, a member of the AFP must apply to an "issuing authority" for a PDO. No preliminary consent is required from the Attorney-General.

In the case of an initial PDO, which may allow, or be extended to allow, detention for up to 24 hours, the issuing authority is in fact a senior member of the AFP itself – a holder of the rank of superintendent or higher. The issuing authority for continued PDOs is different: these orders can only be granted after an initial PDO and can sanction a further period of detention providing that the total period of custody does not exceed 48 hours. In this case, the "issuing authority" is essentially a serving or retired judge who has consented to act in this capacity. A serving judge can only be drawn from federal courts or the Supreme Courts of the states and territories. A retired judge must have served in a "superior court" – any of the courts just mentioned and also state

and territory district courts – for at least five years. Federal magistrates and (subject to some conditions) the President or Deputy President of the Australian Administrative Appeals Tribunal are also eligible for appointment.

According to the Criminal Code, judicial officers are acting in their *personal* capacities and not as members of their courts when they make, extend or revoke a PDO. This is because the Australian Constitution restricts the powers that can be granted to judges as members of their courts. In the *Boilermakers' Case* the High Court interpreted the Constitution as requiring a strict separation of judicial power from the powers held by the parliament and the government.[18] It prohibited federal judges from exercising non-judicial power – and issuing a PDO is not a judicial function; judicial power is traditionally restricted to ordering detention and punishment after a person has been found guilty of a crime. The situation for state and territory judges is more relaxed, but the function must still not be incompatible with judicial power.

One way to avoid a constitutional challenge to these arrangements is for the Commonwealth to be clear that – despite first appearances – it is not granting non-judicial powers to *judges* at all. Rather, being a judge is simply what makes a person eligible to act as an issuing authority. Once the judge has consented to be an issuing authority, he or she is given the power in their private capacity. As an example, the High Court has upheld legislation that conferred on judges in their personal capacities the power to issue telephone interception warrants assisting police with criminal investigations.[19] Basically, the individual concerned is recognised as wearing two different hats. This is what the Commonwealth has sought to do in this instance.

This is a precarious fiction. Using judicial office as a means of identifying potential issuing authorities and then claiming the power is conferred on them as private individuals has an air of artificiality. Moreover, the whole exercise could fall apart if a court decided that exercising non-judicial power as an issuing

authority is simply incompatible with a person's holding judicial office – in other words, that a conflict arises when an individual fills both roles. Given the nature of these orders, the potential exists for this aspect of the PDO scheme to be struck down as unconstitutional. It is for this reason that we find retired judges among the people who are eligible to perform the role of an issuing authority. Because they no longer hold any judicial office, the potential conflict does not apply.

Making an initial or continued preventative detention order: There are two bases on which the issuing authority may make a PDO. These apply to both initial and continued versions of the order. First, an order may be made for the purpose of preventing an imminent terrorist attack. For an order to be made on these grounds, the issuing authority must be satisfied that there are reasonable grounds to suspect that the subject either:

- "will engage in a terrorist act";
- "possesses a thing that is connected with the preparation for, or the engagement of a person in, a terrorist act"; or
- "has done an act in preparation for, or planning, a terrorist act."

The issuing authority must also be satisfied that:

- the preventative order would "substantially assist in preventing a terrorist act occurring"; and
- "detaining the subject for the period for which the person is to be detained under the order is reasonably necessary" for this purpose.

The "terrorist act" referred to here must be one that is both "imminent" and "expected to occur, in any event, at some time in the next 14 days." It is open to question whether those two requirements sit comfortably alongside each other – it might have been simpler merely to have had the latter.

Second, a PDO can be made when it is necessary to detain a person for the purpose of preserving evidence relating to a recent terrorist act, being one that has occurred in the last 28 days. Again, an order can only be made if the issuing authority is satisfied that the period of detention is reasonably necessary for this purpose.

The order must stipulate the name of the person affected, the period during which he or she may be detained, the date and time of making the order and the date and time after which the person may no longer be taken into custody (which can be up to 48 hours after the making of the order), and must provide a summary of the grounds on which the order is made. In practice, this last element may be quite brief since the Code allows the issuing authority to withhold information likely to prejudice national security.

What happens under a preventative detention order?

Division 105 of the Criminal Code affirms that the officer taking into custody or detaining a person under the order has the same powers and obligations as an officer arresting a person for committing a criminal offence. It recognises powers to enter and search premises where the subject of the order is reasonably believed to be, and to conduct a frisk search of that person. At the same time, the officer is obliged to explain to the person as soon as practicable the effect of the PDO and any subsequent extensions of that order. The person must also be supplied with a copy of the order. A failure by police to meet these requirements attracts a maximum penalty of two years' jail.

People detained under these orders may be held in a state or territory prison or remand centre. If the person is under eighteen years of age, he or she cannot be detained with people over that age. Section 105.33 amounts to a guarantee against torture by insisting that a person who is in custody or detained under a PDO:

- "be treated with humanity and with respect for human dignity"; and
- "not be subjected to cruel, inhuman or degrading treatment."

A breach of this section is punishable by up to two years' jail.

A more unexpected limit on what may be done with the detainee comes in section 105.42. Other than verifying the person's identity and ensuring his or her well-being, members of the AFP and ASIO are not allowed to question him or her. This provides a measure of assurance that the PDO scheme will not be used as a general tool for gathering intelligence. Where that is necessary, a separate warrant for questioning (and further detention) can be obtained by ASIO, as set out in chapter 2.

It might be thought that the PDO regime is unnecessary given ASIO's far more extensive powers to detain and question people who may have knowledge of terrorist activities. But it can be argued that the PDO provides a far swifter process for taking potentially dangerous people off the streets for a day or two while the AFP considers laying charges or ASIO prepares an application for questioning.

Contacting others while subject to a preventative detention order: At the time these laws were introduced, much of the criticism was focused not just on their effect but on the very stringent prohibitions they placed on detainees' contacting other people and disclosing the existence of the order. Although this prohibition was relaxed somewhat in the final version of the law, a tension remains between the need to prevent possible terrorists from alerting their co-conspirators and the need to ensure that the powers are not misused under a cloak of secrecy.

As a general rule, a person detained under a PDO is entitled to contact only:

- one family member;
- one housemate (if he or she does not live with a family member);
- his or her employer;
- one employee (if he or she employs people in a business);

- one business partner (if he or she engages in a business with others); and
- any other person the police officer detaining the individual allows them to contact.

This guarantees a right to contact a family member, a housemate and someone with whom the person works. But the only information which may be conveyed to these people is that the detainee is "safe but is not able to be contacted for the time being." That formula has raised eyebrows, with some people suggesting that anyone who received a call from a family member in which those vaguely Orwellian words were uttered would know to head straight to the AFP to ask after their relative. Detainees who are under eighteen years of age may contact both parents or guardians and may receive visits of two hours or more duration.

The Code also recognises a right to make a complaint to the Commonwealth Ombudsman as well as any equivalent state or territory body. Detainees are also entitled to contact a lawyer to obtain advice about their rights under the PDO or to arrange for the lawyer to act for them in proceedings, including those relating to the order. These communications – along with communications with family, housemates and work colleagues – will be monitored by police.

The right of an individual to contact a family member or a lawyer may be subject to any prohibited contact order made by the issuing authority. An AFP member can apply for such an order in any of the following cases:

- "to avoid a risk to action being taken to prevent a terrorist act" or "to prevent serious harm to a person";
- to preserve evidence relating to a terrorist act;
- to prevent interference with the gathering of information about a terrorist act or planning of such an occurrence; or

- to avoid a risk to the arrest of a person for a terrorism offence, their taking into custody under a PDO, or their being served with a control order.

As its name suggests, a prohibited contact order removes the right of a person to contact another person identified by the order.

Disclosing the existence of a preventative detention order: It is a crime, attracting punishment of up to five years' imprisonment, for anyone to disclose the existence of a PDO. This applies not just to the person subject to the order and his or her lawyer, but to others who are involved – including the police officer and any interpreter who has assisted with monitoring contact.

The impact of this prohibition can be illustrated by example. Suppose a couple's seventeen-year-old daughter is taken into custody and detained under a PDO. Using her right to contact her parents to inform them of these bare facts (which, as a minor she is allowed to do), the daughter telephones her father. Under section 105.41(4A), he will be liable for up to five years' jail if he discloses this information to his wife if she has not already had direct contact from the daughter, unless he first informs the AFP of his intention to do so. Under subsection (4) of the same provision, both parents will be liable for the same punishment if they tell other family members – including the girl's siblings – of her situation. The recipients of this news are, in turn, exposed to a jail sentence if they pass the information on.

The apparent purpose of these restrictions is to prevent a prohibited contact order being undermined if the news of the PDO is recounted to other people. But the effectiveness of the offences is open to doubt. The unscheduled disappearance of a member of a terrorist cell is, by itself, likely to be more than enough to alert its other members, and passing on the formulaic message that the person is "safe but is not able to be contacted for the time being" could be enough to indicate that he or she is being detained. At the same time, these provisions throw a heavy veil of secrecy over

state-ordered detention. It is questionable whether the supposed gain is worth that cost.

Scrutiny and compensation

Under the Criminal Code PDOs can be reviewed by the Security Appeals Division of the Administrative Appeals Tribunal. But the Code expressly denies any judicial review of the lawfulness of PDO decisions using the grounds and remedies found in the *Administrative Decisions (Judicial Review) Act 1977*. Nevertheless, other forms of judicial review may still be possible in federal courts under the common law, the *Judiciary Act 1903* and the High Court's jurisdiction to review decisions by Commonwealth officers under section 75(v) of the Australian Constitution.

The Code provides the Administrative Appeals Tribunal with the power to declare that a decision by an issuing authority to make or extend a PDO is void. The fact that it has no jurisdiction to do so while the PDO is in force ensures that the subject's liberty can never be affected by such a finding. But even though the declaration comes after the detention has ceased, it is not without consequence since the tribunal may also determine that compensation is to be paid by the Commonwealth to the individual who was detained.

CONCERNS AND PROBLEMS

Constitutionality

We have already mentioned doubts about the constitutionality of PDOs. These doubts centre on the question of whether serving judges can be granted the ability to issue PDOs in their personal capacities without infringing the Constitution's separation of powers. But the problem is not limited to PDOs. The Commonwealth has run a similar risk by empowering federal courts to make control orders that may amount to house arrest. Making such an order against people without a finding of their criminal guilt is not obviously within the parameters of judicial power. As the High Court's Justice Gummow said in *Fardon v Attorney-General*

(Queensland), exceptional cases aside, "the involuntary detention of a citizen in custody by the State is permissible only as a consequential step in the adjudication of criminal guilt of that citizen for past acts."[20] It is unclear whether this view has the support of a majority of the present High Court, but it certainly has solid precedent and principle behind it. Laws giving courts the power to make control orders may be invalid because they infringe the separation of powers between government and the judiciary.

A different concern arises when control orders inhibit an individual's freedom of political communication. In 1997, in *Lange v Australian Broadcasting Corporation*, the High Court found an implied protection for political speech on the basis that it is necessary for the operation of Australia's system of representative and responsible government.[21] The court's findings in more recent cases have not resolved whether judicial power must be exercised with regard for this limitation. As a result, the new powers to restrict a person's ability to communicate with others may need to be read subject to the constitutional requirement that a basic level of political speech must remain free.

It can also be argued that a freedom of movement and association can be implied from our system of representative and responsible government, and that freedom could constrain the use of control orders. Members of the High Court have argued in favour of the existence of this freedom, but it is a far from settled doctrine.

Criminal responsibility

It is striking that the grounds on which PDOs and control orders can be made are defined as terrorism crimes elsewhere in Part 5.3 of the Criminal Code. For example, a control order can be made if the court is satisfied on the balance of probabilities "that the person has provided training to, or received training from, a listed terrorist organisation." This is very similar to the offences found in section 102.5 of the Code, except that section 102.5 employs the higher criminal standard of proof – that of "beyond

reasonable doubt." Similarly, a PDO may be issued where there are merely "reasonable grounds to suspect" a range of activities that are criminal offences in Division 101.

To hark back to the constitutional question considered above, it might be argued that the ability to make control orders and PDOs neither is, nor is compatible with, judicial power because the same conduct that leads to an order already attracts the operation of that judicial power through specific offence provisions. It might thus be argued that what is occurring in Divisions 104 and 105 must be something else. While the outcome of a constitutional challenge to a PDO or control order is difficult to predict, the existence elsewhere in the Code of a traditional judicial process in respect of the same behaviour may be a relevant consideration.

Quite apart from the constitutional issue, it is worrying that the orders may be used to cover those circumstances where the authorities do not possess sufficient evidence to lay a charge. Both schemes might therefore represent an attempt to avoid the regular judicial procedures for testing and challenging evidence in criminal trials before a person's freedoms are removed. This is clearly so in respect of the PDOs, which may be issued by an individual officer simply on the basis of reasonable suspicion, but also applies to the use of a lower standard of proof by courts charged with issuing control orders. The broad scope of the latter – as well as their longer duration – makes this concern particularly strong.

Support from overseas?

The Commonwealth has frequently suggested that these orders are comparable to counterterrorism initiatives in the United Kingdom, which might seem like a powerful argument in favour of their legitimacy. But there are important differences between the two jurisdictions.

After much debate the British parliament voted in early 2006 to allow people to be detained for up to 28 days. This is not, however, a scheme of preventative detention like Australia's.

British police may detain a person who is reasonably believed to be a terrorist for up to 48 hours for a number of purposes, but the prevention of an "imminent" terrorist act is not one of them. Any extensions of the detention period – in blocks of seven days or fewer, up to the maximum of 28 days – can only be authorised if there are "reasonable grounds for believing that the further detention… is necessary to obtain relevant evidence," whether by questioning or by preservation. Essentially, the British scheme has a strong investigatory purpose and is designed to facilitate the laying of charges. The Australian system of PDOs does not have this focus – it is even illegal for an AFP member to question the person detained.

The British system of control orders bears a stronger similarity to the Australian regime. But the context is still easily distinguished. In the United Kingdom, control orders were introduced after the House of Lords' decision in *A v Secretary of State for the Home Department*.[22] In that case their Lordships declared the indefinite detention of non-citizens suspected of terrorist activities to be a disproportionate and discriminatory departure from the European Convention on Human Rights and the United Kingdom's own *Human Rights Act 1998*. At that time, unlike Australia, the United Kingdom had not comprehensively criminalised actions taken in preparation for a terrorist act. Control orders were seen as a means of filling this gap. The introduction of such an offence by the *Terrorism Act 2006* has led the United Kingdom's independent reviewer of the laws, Lord Carlile, to express a hope that the new laws will be used in preference to control orders where possible because "it is better that sanctions should follow conviction of crime rather than mere administrative decisions."[23]

The force of that comment has been underlined as the validity of the control orders has come under judicial scrutiny. The UK High Court of Justice declared that the process by which a control order was made did not provide a fair hearing. Although the Court of Appeal reversed that decision in August 2006, it did uphold a

judicial finding that certain control orders – which included home arrest for eighteen hours of the day – were an infringement of Article 5 of the European Convention on Human Rights, which prevents indefinite detention without trial. These decisions demonstrate the important moderating effect of formal human rights safeguards in the European Convention on Human Rights. Australia, with no equivalent national law, needs to be wary of unthinkingly adopting similar counterterrorism strategies.

•

The introduction in late 2005 of orders for control and for preventative detention represents a major departure from accepted notions of how Australian law works. While the protection of the community has always been an important element in the criminal justice system, these orders pursue that objective to the detriment of other central values like the principle that people should not be detained without trial or their liberty restricted without a criminal conviction.

As nineteenth-century English writer A. V. Dicey emphasised, the rule of law *must* mean that while a person may be punished for a breach of the law, he or she should not be punished for anything else. The two divisions of the Criminal Code described in this chapter depart from this fundamental concept of our legal tradition.

CHAPTER 4

Shades of grey: freedom of speech

In Australia we take freedom of speech for granted. After all, it is one of the bedrocks on which our democracy is built, an assumption that underpins both our law and our politics. This is consistent with our image of Australia as a democratic nation with a proud history of political freedom. But even something as fundamental as freedom of speech can come under threat during times of war. At such times governments commonly seek greater power to control not just what people do, but also what they say.

The laws examined in this chapter, especially the new sedition law enacted in late 2005, have excited more public debate than any of the other counterterrorism laws. While we recognise that some limitations on freedom of speech can be justified on some occasions, the critical questions are: when and by how much? Some of the laws passed since September 11 restrict free speech as a reasonable measure to protect Australians from terrorism; others are far harder to accept.

FREE SPEECH AND NATIONAL SECURITY

As with other human rights, there must be some give and take between freedom of speech and the need to protect the community from terrorism. The difficulty lies in deciding where to draw the line. Laws that clamp down too far on speech may undermine

the very democracy those laws are designed to protect. The object is not national security at any cost, but the security of our democratic system of government and the freedoms that underpin our way of life. Bad laws that go too far may even make the problem of terrorism worse by fostering a sense of grievance and alienation among people who already feel excluded or have experienced discrimination. Getting the balance right is a delicate task when terror laws affect fundamental political freedoms and can be used by a government to prevent public scrutiny of its work. Indeed, when free speech is at stake it is usually better to err on the side of caution.

There is a commonsense approach to assessing such laws. First, freedom of speech should only be limited where it can be demonstrated that the restriction will actually help to lessen a harm like terrorism. Second, the restriction on speech should be proportionate to the harm that is to be prevented (for example, a law could not be justified if it banned expression or criticism of the government in order to achieve a minor outcome). Third, where both of these conditions are met, the actual limitation on speech should be the least restrictive means of achieving the goal. Under this test, laws that are ill-directed, overly broad or more stringent than is necessary cannot be justified.

In other nations with a charter or bill of rights, an approach like this is often used by the courts to assess laws. It enables bad laws to be identified, and in some cases even struck down. In Australia, bad laws can continue to operate without this type of scrutiny. The best we have is not a national charter of rights but an implied freedom of political communication derived from the Constitution by the High Court. The scope of that implied freedom is relatively narrow: it does not cover a wide range of speech that would be protected in other nations (such as works of art and academic scholarship) unless it can be shown to have a political dimension. The implied freedom has rarely been applied by the High Court, and it is no substitute for the scrutiny usually possible under an express right of free speech in a charter of rights.

NEW LAWS SINCE SEPTEMBER 11

Many of Australia's new anti-terrorism laws have a minor or incidental impact on freedom of speech. For example, the offences examined in chapter 1 – the basic offences under the new laws – criminalise behaviour that may involve expression and attempts to influence political views. This is hardly surprising when the very definition of terrorism is centred around an action being done "with the intention of advancing a political, religious or ideological cause." Offences that may affect speech include the bans on providing or receiving training connected with terrorist acts and on making documents likely to facilitate terrorist acts. Both offences will inevitably involve an element of oral or written expression. These offences can be justified even though they affect freedom of speech. They are not directed at limiting speech but at other objects entirely, such as banning training or preventing terrorist attacks, and they go no further than is necessary to meet the main objective of protecting the community from harm.

A law that has an incidental impact on expression, but which may be more problematic, is that which allows control orders to be imposed on people, including orders that may limit the ability of people to communicate with others (see chapter 3). Whether or not such a control order can be justified would need to be examined on a case-by-case basis.

We examine below new Australian counterterrorism laws that more directly prohibit some kinds of speech. Like some other nations, Australia has seen fit to target not only terrorist acts but also the speech connected with such acts. In the United Kingdom, for example, a law passed after the 2005 London bombings bans the "glorification" of terrorist acts, with a penalty of up to seven years in jail.[24] Under that law it is no defence to argue that no one was encouraged or induced by the statement to commit or prepare for a terrorist act.

That law, as well as the Australian laws examined below, can have a major impact on what people can say. They can also frustrate

the public's ability to hold the government to account. The laws raise difficult questions about how far Australia should go in the "war on terror" and the extent to which the way we are fighting that war is weakening the democratic system that the law is meant to protect.

ADVOCATING TERRORISM

In chapter 1 we considered how the Criminal Code enables terrorist organisations to be banned. A body can be proscribed for being a terrorist organisation not only because the government believes that it is engaged in preparing, planning or performing a terrorist act, but also because it "advocates the doing of a terrorist act (whether or not a terrorist act has occurred or will occur)." In other words, organisations can be banned not just for their actions but also because of what is said on their behalf. Once an organisation is banned, severe penalties of up to 25 years in jail apply to people who are members of the organisation or provide support for its activities.

Section 102.1(1A) of the Criminal Code states that an organisation advocates the doing of a terrorist act if:

> (a) the organisation directly or indirectly counsels or urges the doing of a terrorist act; or
>
> (b) the organisation directly or indirectly provides instruction on the doing of a terrorist act; or
>
> (c) the organisation directly praises the doing of a terrorist act in circumstances where there is a risk that such praise might have the effect of leading a person (regardless of his or her age or any mental impairment… that the person might suffer) to engage in a terrorist act.

This definition is extremely broad. Part (c) is particularly problematic. It does not require an organisation to encourage someone to undertake a terrorist act, but is far more indirect. It extends to where an organisation "praises" someone else's terrorist act and

there is a mere "risk" that this might lead another person again to commit such an act (including where that person is very young or of unsound mind). An example could be where an organisation's executive or membership praises Nelson Mandela's resistance against apartheid in South Africa. As we saw in chapter 1 his struggle would amount to terrorism under Australian law, which provides no exceptions for legitimate acts of liberation or for resistance against dictatorship or other forms of oppression. There is a risk that praising Mandela's fight could encourage someone else in Australia or elsewhere in the world to take up arms against a similarly abhorrent regime. Such speech is itself sufficient to fit within the conduct targeted by the law.

Many other potential examples come to mind, such as where someone praises past liberation struggles in East Timor or against a colonial power, or current battles in West Papua, the Middle East and parts of Africa. Whatever the merits or otherwise of these struggles, the Australian law is far too broad. It is a blunt instrument for dealing with sensitive matters about which Australians may legitimately disagree.

An earlier draft of the British "glorification" law sought to avoid this problem by stating that the glorification of actions that occurred over twenty years before was only an offence if the action was specified in an order by the Secretary of State. But drawing up such a list proved impossible, and only opened up a larger, unresolvable debate about the use of violence. In any event, it ought not to be up to the government to decide which historical events we can say were justified and which were not.

Banning terrorist organisations for their advocacy is not only hazardous because it affects what an organisation can say. It is also of concern because it affects people who did not say the words. Even if they disagree with what was said, other people can be jailed because of their association with the body. Proscribing speech is troubling enough without also punishing people who have not made a statement but who are members or supporters of the same organisation. This is an extraordinary extension of

the power of proscription and of criminal liability since it collectively punishes members of groups for actions by associates who are beyond their control.

While it may be acceptable to ban groups that actively engage in or prepare for terrorism, it is not justifiable to ban an entire group merely because someone affiliated with it praises terrorism. It is well accepted that speech that directly incites a specific crime may be prosecuted as an incitement. It is quite another matter to prosecute a third person for the statements of another, especially when such statements need not be directly connected to an offence.

ASIO AND OPERATIONAL INFORMATION

In chapter 2 we discussed the new powers conferred on ASIO. The most contentious of these is the detention of people, including Australian citizens, not because they are suspected of any crime or involvement with terrorism but because they may have information that can assist ASIO with its intelligence-gathering. The problems with this law are magnified by a provision that limits speech about the exercise of that power.

The *Australian Security Intelligence Organisation Act 1979* makes it an offence to disclose "operational information" obtained indirectly or directly through the exercise of a questioning warrant or a questioning and detention warrant within two years of the expiry of the warrant. Operational information is defined very widely to include information that ASIO "has or had" and to cover "an operational capability, method or plan." Revealing such information can incur up to five years' imprisonment. While the warrant is in force, it is also an offence to disclose even the mere fact that someone has been detained or questioned, or any other matter relating to the content of the warrant or the questioning or detention of the person. There are no exceptions for fair reporting or if the information is published as part of a media story that reveals that ASIO has abused its powers or mistreated detainees. The limited exceptions include

disclosures to a lawyer for the purposes of obtaining legal advice about an ASIO warrant or obtaining legal representation in proceedings for a remedy related to a warrant.

It is understandable, and justifiable, that the government would seek to protect some of ASIO's activities from public view. Much of the work of the organisation depends on its ability to maintain secrecy, and this extends to the tactics and methodologies used by ASIO to combat terrorism. But in providing a blanket ban on the disclosure of "operational information" the law goes too far. The definition of "operational information" is so broad, and so vague, that it is unclear what can be said about ASIO's activities under its new powers. For example, how will a person who receives information indirectly, such as a journalist, know whether it is information that ASIO "has or had"?

It would be better to narrow the prohibition on what can be said and give ASIO the power to seek an order preventing the disclosure of other information. As it is, the law prevents disclosure not only of information that ought to be kept secret but also of a potentially far greater range of material, including detail that the public needs to scrutinise the work of ASIO and of the government.

This problem is not solved by the exception at the end of the law, which states that it does not apply "to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication." This clause does nothing to indicate in any meaningful way what can be said without breaching the law. (At the very least, it could require expensive advice about constitutional law to form a judgement.) It merely seeks to prevent the provision from being struck down by the High Court if it did breach the implied freedom.

The effect of this law is that if someone is mistreated while being detained we may have to wait two years or more to find out. Combined with the cloak of secrecy that surrounds so many of the new terrorism laws, and the fact that it is a crime to identify an ASIO officer, this is a grave threat to the accountability of government.

SEDITION

The offence of sedition traditionally involved words or acts that incited discontent or rebellion against the monarch or the authority of the state. It developed as part of the ancient law of treason, then emerged as a distinct offence in the United Kingdom in the early seventeenth century. Australia inherited the British common law of sedition, which was codified in a 1920 amendment to the federal *Crimes Act 1914*. Since then, though, the law of sedition has largely been discredited, mainly because of the use to which the laws were put. Sedition laws have been used against dissident figures like Mahatma Gandhi and Nelson Mandela and, in Australia, against members of the Australian Communist Party.

In late 2005, in the wake of the London bombings, the Australian parliament passed a new sedition law. Exactly how the new law will make Australians safer from terrorism has not been made clear. Indeed, there is a real risk that the law will further ostracise members of those communities that feel, rightly or wrongly, that they are already the target of government action. There is also the potential that the law will push speech that promotes political violence underground rather than bringing it out into the open to be contested and exposed in public debate. Banning speech can even make the ideas it embodies more popular to some.

The new sedition law generated significant political and community opposition. In the artistic community, for example, the Footlice Theatre Company in Newcastle examined the sedition laws in a sketch-style show, *Myths, Media and Misfits*, and, in Sydney and Melbourne, humorist Wendy Harmer hosted an anti-sedition concert called *Sedition!*.

Parliament nonetheless acted with haste and passed the law so that it would be operating, as the government desired, by Christmas 2005. The law removed the existing sedition offences from the *Crimes Act* but retained offences for involvement with unlawful associations, which include an association that "advocates or

encourages the doing of any act having or purporting to have as an object the carrying out of a seditious intention."

The law created new sedition offences in section 80.2 of the Criminal Code punishable by up to seven years in jail. They apply to anyone, Australian or not, anywhere in the world, but the Attorney-General must consent to the prosecution of an offence. The offences include situations where a person urges:

- "another person to overthrow by force or violence" the Constitution, a state, territory or Commonwealth government, or the authority of the Commonwealth government;
- "another person to interfere by force or violence with lawful processes for an election of a member or members of a House of Parliament";
- "a group or groups (whether distinguished by race, religion, nationality or political opinion) to use force or violence against another group or other groups (as so distinguished); and the use of the force or violence would threaten the peace, order and good government of the Commonwealth";
- "another person to engage in conduct" with the intention that the conduct "assist an organisation or country" that is "at war with the Commonwealth, whether or not the existence of a state of war has been declared" and is specified by proclamation to be "an enemy at war with the Commonwealth"; or
- "another person to engage in conduct" with the intention that the conduct "assist an organisation or country" that "is engaged in armed hostilities against the Australian Defence Force".

A person does not commit an offence if he or she acts in "good faith" in a set of specified circumstances – pointing out errors in legislation, for example, or urging someone to attempt lawfully to bring about a change to a law, or publishing a report or commentary on a matter of public interest. If a person is charged with a sedition offence, he or she can exercise any of

these defences by pointing to evidence that suggests there is a reasonable possibility that the acts were carried out in good faith. The prosecution will then have to refute this beyond reasonable doubt. The Criminal Code also sets out matters that the court can consider in deciding whether the acts were done in good faith, including whether the acts were done with the intention of assisting an enemy or another country that is engaged in armed hostilities against Australia.

While the law of sedition has been "modernised" in the 2005 legislation, it still provides few exceptions. No specific defences are given for many forms of communication, including academic or scientific discussion. It even fails to protect satire or comedy, a very Australian way of dealing with something as difficult and troubling as the "war on terror." Black humour, typified in the way ABC Television's *The Chaser's War on Everything* uses the words and images of Osama bin Laden, has the potential to become a criminal offence.

Attorney-General Philip Ruddock has said he will not apply the sedition law in such cases. But there is no way of knowing how this or future governments will use the law, and Mr Ruddock's undertaking also ignores the larger problem of self-censorship. Sedition and other laws constraining speech inevitably have a "chilling" effect on what we say. Artists and commentators are now less likely to use robust critical speech about the "war on terror" or other sensitive topics. When people do not have free on-the-spot legal advice, they may not speak for fear of the consequences.

When the sedition law was passed in late 2005, it was widely believed to be flawed. The law punishes people with up to seven years' jail not for what they do but for what they say, and it is too broad both in the speech that is banned and in having too few defences. At the time, and under pressure from members of its own backbench, the government accepted some changes to the law, including the introduction of a defence for publishing in good faith on a matter of public interest. Even then, the law was

far from acceptable to many and needed more time to be scrutinised and drafted more carefully. Yet parliament passed the law anyway. It was a particularly poor example of law-making. There are very few other examples where a law targeting something as fundamental as political speech has been enacted as quickly as this, and despite the fact that people from all sides of politics recognised that it needed to be changed.

The compromise reached at the time was that the new sedition law would be referred to the Australian Law Reform Commission. When the commission released its discussion paper in May 2006 no one was surprised that it proposed substantial changes. A key finding was that the term "sedition" should be removed from the statute book. The commission recognised the discredited nature of such laws and the problems created by reincarnating them in a modern guise. It suggested narrower "offences against political liberty and public order" that would criminalise speech where it could be proved beyond reasonable doubt that a person had intentionally urged others to use force or violence, and intended that this force or violence would occur.

The commission recommended a redraft of the offences to ensure that legitimate forms of communication – including artistic speech, commentary and academic scholarship – were protected. Instead of offering "in good faith" defences the legislation would require the court to consider such factors in establishing an intention for force or violence to occur as an element of the offence itself. The commission also suggested that the offence of urging a person to assist an enemy or country engaged in armed hostilities against Australia should be repealed, as it "could be interpreted or applied to proscribe legitimate political protest, and punish merely verbal encouragement or support for those in conflict with Australian government policy."[25]

At the time of the release of the discussion paper, Attorney-General Philip Ruddock said that if he could remove the reference to sedition while "retaining the full intent of the original legislation – that is, targeting those who would urge the use

of force or violence in our community," then he would seriously consider such a recommendation.[26] The commission has since sought comment on its proposals with a view to writing its final report to the government.

•

Freedom of speech is a casualty of the laws passed in Australia in the name of the "war on terror." While some of these laws only have a minor and justifiable impact on the freedom, others are of great concern. People can now be jailed not just for their acts but also for what they say. Not only that, people can be jailed because of what *someone else* has said when they are both members of the same organisation.

Fortunately, there have been no prosecutions under these provisions. But the very fact that they are part of our law is inconsistent with our aspiration to remain a free, open and democratic society. Such laws could be used inappropriately in the future by an unscrupulous government. The laws also set an unfortunate precedent by trading away free speech in overly broad laws that may not even help to reduce the threat of terrorism. With the gate seemingly now open to laws that restrict speech directly, it is possible that Australia will see more laws that are inconsistent with this fundamental freedom.

The laws passed since September 11 demonstrate how fragile freedom of speech is in Australia. They expose how we assume, rather than actually protect, that freedom. To an even greater extent than in nations such as the United Kingdom and the United States, our law has come to reflect President George Bush's maxim that "you're either with us or against us." When it comes to acts of political violence, there is now less space for comment by the critical writer or thinker. Such a person may see shades of grey rather than black and white or right and wrong. We do not live in a black and white world.

CHAPTER 5

Prosecuting terrorists

How have Australian courts applied the new anti-terrorism laws? In this chapter we discuss several of the small number of prosecutions of people charged with terrorism crimes under Australian law. We also examine the *National Security Information (Criminal and Civil Proceedings) Act 2004*, which is designed to prevent sensitive national security intelligence from being disclosed in the trial of a person on terrorism offences. This Act requires a defendant's lawyer to obtain a security clearance from the Attorney-General's Department to gain access to the information needed to represent his or her client. An even more controversial aspect of the law is the power it gives the Attorney-General to direct that a court be closed to the public and evidence barred on the basis of national security.

TERRORISM TRIALS

Since July 2002, when the first anti-terror laws came into force, 28 people have been charged with a range of terrorism offences under Part 5.3 of the Criminal Code (which we discussed in chapter 1). A small number of charges have also been laid under other criminal provisions, including for the offence of knowingly making a false or misleading statement when questioned by ASIO (chapter 2). Most of these matters are yet to go to trial. Others have commenced but are still concerned with preliminary questions of a technical or procedural nature. The three cases below have all gone to trial.

Zeky Mallah

Mallah is a young Australian citizen who applied to the Department of Foreign Affairs and Trade for an Australian passport. This brought him to the attention of ASIO, which interviewed him. His application was refused on the ground that he was assessed as likely to engage in conduct prejudicial to the security of Australia or a foreign country. He unsuccessfully sought a review of that decision by the Administrative Appeals Tribunal. Over the course of these events, he developed an animosity towards the government departments involved.

As his defence counsel, Phillip Boulten SC, described it, Mallah became something of a minor celebrity after his flat was raided and the NSW police charged him with illegal possession of a gun.[27] His apparent enjoyment of this attention made him susceptible to an undercover operation by the NSW Police Counter Terrorist Co-ordination Command.

A police officer posing as a journalist met with Mallah for several discussions, which the latter believed would lead to media coverage. Mallah revealed to the "journalist" his plan to enter an ASIO or Department of Foreign Affairs and Trade building with a weapon and kill members of their staff. The "journalist" learned that Mallah had recorded a video message explaining these planned actions. Mallah supplied the video tape for $3000, whereupon he was charged under section 101.6 of the Criminal Code with doing an act in preparation for a terrorist act. Subsequently, another charge was laid under this provision in relation to Mallah's earlier acquisition of the rifle. He was also charged with the non-terrorism offence (under section 147.2) of making a threat to another to seriously harm an officer of the Commonwealth. Mallah pleaded guilty to this last charge for which he was sentenced to two and a half years' jail.

The jury in his trial found Mallah not guilty on both of the charges under section 101.6. His defence argued that Mallah had conducted the conversations with the "journalist" simply to gain further attention and profit; he had no serious intention of car-

rying out the "plan" which formed the basis of these discussions. According to the defence, Mallah's decision to purchase the weapon was motivated by fears for his own safety because he had received threats of harm after the earlier media coverage.

Boulten's remark that the jury's verdict "reflected a widespread impression that the authorities had over-charged this young man" seems a sound assessment.[28] It must be borne in mind that a conviction under section 101.6 comes with a possible penalty of life imprisonment – a factor that may account for the jury's unwillingness to convict. Mallah may have been many things, but it was questionable that he posed such a threat to Australia's national security that he should be charged under several of the Code's strongest terrorism offences.

When the Commonwealth Director of Public Prosecutions, the DPP, recommended to the Security Legislation Review Committee that the definition of "terrorist act" in the Criminal Code be watered down, it used the failed charges against Mallah as supporting evidence. The DPP argued that it should no longer be necessary to prove an intention to "advance a political, religious or ideological cause" in order to obtain a conviction. Arguably, it was on this element that the prosecution came unstuck in its case against Mallah, since his hostility towards the government arose from his personal experiences rather than any broader cause. The DPP favoured a definition that required only proof that the defendant had the "intention of coercing or influencing by intimidation a government, or intimidating the public or a section of the public."

Some countries do have laws in which the definition of terrorism is not restricted by reference to a motivating belief. But those laws, and the DPP's proposed definition, are problematic because they fail to identify the very factor that distinguishes terrorism from other crimes. As the case of Mallah itself showed, there are other laws covering dangerous or threatening behaviour. We should be wary of an over-eagerness on the part of authorities to find terrorist acts where once they would simply have seen ordinary crimes.

Joseph Thomas

Thomas – nicknamed "Jihad Jack" – was charged in Victoria with offences under sections 102.6 (intentionally receiving funds from a terrorist organisation) and 102.7 (intentionally providing support to a terrorist organisation) of the Criminal Code. He was also prosecuted for possession of a false passport, which was an offence under section 9A of the *Passports Act 1938*.

The prosecution's case was based on evidence concerning Thomas's activities in Pakistan from 2001 to 2003. It was alleged that he had trained at an Al Qa'ida camp – though it should be noted he was not charged with the offence in section 102.5 which relates to such activities – and then made himself available as a "human resource" prepared to engage in a terrorist act. Thus, the main charge against Thomas was that he had provided support to a terrorist organisation in breach of section 102.7. On this the Victorian Supreme Court jury acquitted him.

He was, however, convicted on the other two charges. The prosecution satisfied the jury that Thomas received money from Al Qa'ida to pay for his airfare back to Australia and that he had fraudulently altered his passport to conceal the length of his stay in Pakistan. In March 2006, Thomas was sentenced to five years' imprisonment for the former and two years' for the latter, to be served concurrently.

During the trial, Thomas sought to challenge the prosecution's reliance on an alleged admission he made to the Australian Federal Police, the AFP, while he was held without charge by the Pakistani authorities. Thomas was held in a kennel-like cell for approximately two weeks and was without food for about three days. He was assaulted and threatened with torture, indefinite detention and execution. He was told his wife would be raped. Interrogators, including Australians, also offered Thomas inducements for his cooperation. Contrary to guarantees in the *Crimes Act 1914*, he was not able to have a lawyer present for these interviews.

Despite these circumstances, Justice Cummins admitted as evidence in Thomas's trial an interview he had had with the AFP

in Pakistan. Cummins found that because this interview occurred a few weeks after those earlier threats and inducements Thomas's statements would not have been coloured by them. The Court of Appeal disagreed. In August 2006, it found that Thomas's detention, the inducements and threats, and the prospect of indefinite detention weighed heavily on his mind at the time of the interview. His admissions were not voluntary because Thomas effectively did not have a free choice to speak or be silent. The court also criticised the absence of a lawyer during the interview. The court quashed the conviction but, as we write, had yet to decide whether to accept the DPP's proposal for a retrial on the basis of statements made by Thomas in an interview on ABC's *Four Corners*.

Less than ten days after his convictions were quashed, but before the Court of Appeal had decided whether he should stand trial again, the AFP obtained an interim control order against Thomas. This was the first control order issued in Australia. The order means that Thomas must remain in his home between midnight and 5am every night and report in person to the police three times a week. He can only use identified telephones and internet services, and must not communicate with a member of a terrorist organisation or 50 specified people, including Osama Bin Laden. The AFP is seeking to have the control order confirmed so that it will apply for up to a year.

Quite apart from the specific facts of the Thomas trial, it is obvious that the circumstances under which evidence is gathered will be a major issue in many terrorism cases. The prosecution will need to ensure that its case stands up under the traditional standards of Australian justice.

On this point the fate of David Hicks, the Australian citizen held at Guantanamo Bay, is relevant. After much delay, Hicks was charged with a number of offences that were to be heard by a specially constituted military tribunal. In mid 2006 the US Supreme Court declared those bodies to be unlawful and the Bush administration announced that it would work with Congress to devise

an alternative means of hearing charges against the detainees, whom it has labelled "enemy combatants." Meanwhile, Hicks has already been held for almost five years. The US and Australian governments are determined that Hicks will not be tried by an ordinary court, perhaps because such a court would not accept the evidence against Hicks as admissible or sufficient to convict him of any crime.

The other Australian held at Guantanamo Bay, Mamdouh Habib, was released after many months of detention and returned to Australia quite unexpectedly in 2005. He has since claimed that he was subjected to "extraordinary rendition" – essentially the practice of sending an individual to another country in order to evade restrictions on the use of torture in questioning. Habib has not been prosecuted for committing any terrorism crimes. If the only evidence against him was procured by such methods then this is not surprising.

The ways in which evidence is gathered and defendants questioned affect not only the rights of the accused but also the strength of the prosecution case. Securing a conviction can be difficult or even impossible in the face of allegations of impropriety or abuse. Convictions reached in open court on the basis of strong evidence, by contrast, will enhance public confidence in the justice system. The community must be assured that the courts are exercising their powers in line with accepted notions of fairness and justice – even, or perhaps especially, when people are charged with crimes as serious as terrorism.

Faheem Lodhi

The prosecution's case against Faheem Lodhi was that, using a false identity, he engaged in activities in preparation for a terrorist act. Summarising the evidence against his client, Phillip Boulten SC wrote that Lodhi was detected "purchasing maps of the electricity grid, making enquiries about the availability of chemicals, downloading aerial photographs of Victoria Barracks, Holdsworthy Barracks and HMAS Penguin and acquiring a large

quantity of toilet paper."[29] (The toilet paper was allegedly for the production of nitrocellulose.)

So far Lodhi bears the distinction of having been charged with the most offences under Part 5.3 of the Criminal Code. He was charged with:

- possessing a thing connected with preparation for a terrorist act – section 101.4;
- collecting documents connected with preparation for a terrorist act – section 101.5;
- making a document connected with preparation for a terrorist act – section 101.5;
- doing an act in preparation for a terrorist act – section 101.6; and
- giving false or misleading answers under an ASIO warrant – section 34G, *Australian Security and Intelligence Organisation Act 1979* (five counts).

As discussed in chapter 1, offences were amended in late 2005 to make it clear that the prosecution need not show that the activity in question was connected to a *specific* terrorist act. Lodhi had already been charged under these sections before they were altered, but the NSW Supreme Court suggested that this was of little consequence. According to Chief Justice Spigelman, even before the clarification the offences applied to "conduct where an offender has not decided precisely what he or she intends to do."[30]

The challenge that this "special, and in many ways unique, legislative regime" (to use Chief Justice Spigelman's description) poses to our traditional understanding of what constitutes a crime was discussed in chapter 1.[31] Of course, requiring the prosecution to satisfy the jury of every minute detail of a terrorist plot would be unrealistic. But when the offences relate merely to possession or some preparatory act, a more reasonable specificity would normally be required.

Lodhi was found guilty of all charges under the Code except that of making a document connected with preparation for a terrorist act. His sentencing was postponed for the judge to take account of special provisions requiring that people convicted of terrorism offences serve 75 per cent of their jail term before being eligible for parole. Lodhi was sentenced to twenty years in jail with a non-parole period of fifteen years. He is still facing trial for the charges under the *ASIO Act*.

The Lodhi trial was a notable win for the DPP after less convincing outcomes in the Mallah and Thomas cases. But, even so, some people were quick to call for changes to the law to improve the prosecution's chances. By far the most concerning of these was the suggestion that juries should not be used in terrorism trials. The jury in the Lodhi case had deliberated for several days, which led to speculation that it might fail to reach a verdict – although that, of course, was not the outcome. All the evidence from the three cases discussed here is that the courts have been conscientiously served by juries. In the present climate of fear about terrorism it would be all too easy for jurors to rush to convict someone alleged to have been planning these crimes. That has not occurred. Instead, juries have taken their time and weighed the evidence before reaching their verdicts.

Finally, it is worth noting that the Lodhi trial was frequently interrupted by procedural hearings about the admissibility of evidence under new rules that parliament had introduced in 2004. These are found in the *National Security Information Act*, the NSIA, and highlight the tensions between open justice and the Commonwealth's attempt to prevent the disclosure of information that might be prejudicial to national security.

THE NATIONAL SECURITY INFORMATION ACT

For reasons of "national security" the government is anxious to control what information emerges in an open court during a terrorism trial. The NSIA was passed to prevent any material that might endanger Australia's "defence, security, international rela-

tions or law enforcement interests" from being made public in the course of a trial. Attorney-General Philip Ruddock said that the law was needed to protect "people who may have given information for intelligence purposes," for example, or to avoid warning people "to change their behaviour to avoid inquiries or detection." He also said that much of Australia's intelligence "comes from agencies abroad who say that this is our information and we will only share it with you if it's dealt with appropriately."[32]

These are strong reasons, but it is important not to lose sight of the fundamental principle that an accused is entitled to know the details of the case against him or her. Our system of justice is famously an open and transparent one. The NSIA attempts to strike a balance between those considerations and the need to preserve valuable intelligence. Whether it succeeds is a matter of continuing debate.

Scope

As originally enacted, the NSIA applied to any criminal proceeding in any court exercising federal jurisdiction in relation to Commonwealth offences. It covered all stages of the proceeding from the charge through to appeal. In 2005 an amendment was made to extend its operation to civil matters. In these cases, some of the rules were relaxed. For example, in a civil case a party may personally apply for a security clearance to view sensitive information, something that is not permitted in criminal proceedings. The Commonwealth DPP has called for the NSIA to be further extended to state and territory prosecutions.

Controlling information

Obligation to notify: The NSIA sets down these obligations on the legal counsel in federal proceedings:

- If either the prosecutor or the defendant knows or believes that he or she will disclose information which relates to or

may affect national security, he or she is required to notify the Attorney-General as soon as possible. This can happen before or during the trial.

• The same responsibility also rests on the prosecutor and defendant if they think that a witness they intend to call will disclose such information either "in giving evidence or by his or her mere presence."

• If a witness is asked a question in giving evidence and the prosecutor or defendant thinks that the answer will disclose such information, he or she is required to inform the court. A closed hearing will then be held, where the question will be answered in writing. This answer is shown to the prosecutor who is then required to notify the Attorney-General if he or she thinks the answer might relate to or affect national security.

A failure to comply with these requirements is punishable by imprisonment for two years.

The Attorney-General's certificate: On notification, the court must adjourn until the Attorney-General has either issued a certificate to the prosecutor or defendant or advised the court of a decision not to do so. The Attorney-General has extraordinarily broad powers to determine how he or she will respond to the notification:

• If the Attorney-General considers that the disclosure would prejudice national security he or she may issue a certificate to the potential discloser of the information directing that person not to reveal it.

• If the sensitive material was to be tendered as a document, the Attorney-General may supply the potential discloser with a copy from which certain or all information has been deleted accompanied by a summary of the information it contained. If, on the other hand, the information would have been given in some other form, the Attorney-General may provide a

written summary or statement of the facts, and this must be used as a substitute.

• Where the "mere presence" of the witness risks the disclosure of information, the Attorney-General may issue a certificate which states that the witness is not to be called.

These powers can be exercised without a notification if for any reason the Attorney-General expects that the prosecutor, the defendant, or the mere presence of a witness will disclose sensitive information. Disclosing the relevant information either after notification, but before the Attorney-General issues a certificate, or contrary to the terms of such a certificate, is punishable by imprisonment for up to two years.

Closed hearings: Any certificates issued by the Attorney-General must be considered by the court in a closed hearing. Ideally, this would occur before the start of the trial. But certificates may be issued at any stage of the proceedings, necessitating an adjournment while the court considers the effect of the certificate on the evidence in question. The Lodhi case was frequently slowed down by closed hearings of this sort.

The only people allowed to be present for these closed hearings are:

• the magistrate or judge/s;

• court officials;

• the prosecutor;

• the defendant;

• the legal representative of the defendant;

• the Attorney-General (and his or her legal representative) if he or she has decided to intervene in the matter; and

• any witnesses allowed by the court.

The court is authorised to exclude the defendant from these hearings if it decides that he or she may be exposed to sensitive

information. The defendant's legal representative or court officials may also be excluded if they have not been given a security clearance and it is likely that national security would be prejudiced if they were to hear the information. But if either the prosecution or the Attorney-General argues for the non-disclosure of the information, the defendant and his or her legal representative must be given the opportunity to make submissions regarding this argument. Their capacity to do so would be significantly hampered if they have been barred from the hearing, which also means they would not be entitled to a copy of the record of the hearing. Clearly, security clearances are vital to effective legal representation. This aspect of the NSIA will be further considered below.

Court orders: After holding a closed hearing the court must make an order as to whether the evidence may be disclosed in full or subject to restrictions. Similarly, the court decides whether to allow or prevent the calling of a witness whose appearance has been challenged as a threat to national security. In making whatever order it settles on, the court must consider:

- whether, having regard to the Attorney-General's certificate, there would be a risk of prejudice to national security if the information were disclosed or the witness called; and
- whether the order would have a substantial adverse effect on the defendant's right to receive a fair hearing, including in particular the conduct of his or her defence.

The Act specifically states that the Attorney-General's certificate is to be given the "greatest weight" of these two considerations. While the NSIA leaves the final order in the court's hands, it guides its discretion in favour of the government.

The court must supply reasons to the person who is the subject of the order, the prosecution, the Attorney-General (if he or she intervened in the closed hearing), the defendant and his or her

legal representative. Both parties have the right to be granted an adjournment to decide whether to appeal the order to a higher court. Contravening the terms of the court's order is, like all other offences in this part of the Act, punishable by up to two years' jail.

Security clearances

The negative impact of the NSIA restrictions on a defendant's case may be minimised if his or her counsel has received a security clearance from the Attorney-General's Department. This will enable the defendant's lawyer to be present at any closed hearings of the court and to hear why the evidence raises concerns about national security. Only by being present can the defence hope to challenge the basis of the Attorney-General's certificate and exert influence over the court's order.

The Act says that if the Attorney-General notifies the defendant's advocate before or during a trial that an issue of national security is likely to arise, the lawyer may apply for a security clearance. The court must defer or adjourn the proceedings until this has been granted or another legal representative of the defendant succeeds in gaining clearance.

Members of the legal profession have argued that this requirement is an intolerable intrusion into their private affairs and impairs the right of defendants to choose their legal representation freely. There is also concern that the grounds on which a clearance is denied will not be revealed and thus cannot be challenged.

In the United Kingdom, the problem of trusting defence lawyers with sensitive information has led to the creation of "special advocates." This is a small team of security-cleared lawyers appointed by the Attorney-General. This more formal approach also has its problems. Several of the "special advocates" have resigned and declared the system flawed. The system certainly reduces a defendant's choice of lawyers, but its chief deficiency lies in the the fact that advocates may not discuss the protected information with their clients and so are hampered in responding to specific allegations. Restrictions on access to infor-

mation are one concern, but the greater problem may be the impact on free and frank communication between defendants and their lawyers.

•

Terrorism trials throw up challenges that do not exist when the courts deal with other crimes. It is one thing to criminalise preparatory actions that are not yet linked to any particular intention to commit a terrorist act – it is another to mount a successful prosecution. The small number of cases concluded in Australia provide some insight into the challenges for courts in working with the new provisions of the Criminal Code.

The many cases yet to be heard will further expose the difficulties that face both the prosecution and the defence. Many problems will arise out of the procedural obligations and constraints imposed by the NSIA during terrorism trials. That Act will pose particular problems for the defence. While driven by understandable concerns about preserving national security, the law prioritises the Attorney-General's opinion over the right of defendants to receive a fair trial in which the evidence against them is clearly stated and can be directly challenged. This is always going to be a difficult balance to strike. But when the effect of the NSIA is considered in combination with the very broadly drafted terrorism offences the odds appear to be too heavily stacked against the defendant.

CHAPTER 6

What price security?

In an era punctuated by terrorist attacks in New York and Washington and in Bali, Madrid, London, Mumbai and elsewhere, new laws were needed in Australia to deal with terrorism. They were necessary to signal that we reject such violence and to ensure that our police and other agencies have the powers they need to protect the community. A legal response was also needed to fulfil our international obligations as a member of the United Nations. For example, Resolution 1373 of the United Nations Security Council, made on 28 September 2001, determines that governments shall take "the necessary steps to prevent the commission of terrorist acts."

Governments across Australia deserve credit for recognising this need, and parliaments for passing laws that, among other things, make terrorism a crime. In hindsight, our legal system prior to 11 September 2001 reflected complacency about the potential for political violence in Australia and the region. New Zealand, by contrast, has had terrorism laws since 1987.

While Australia needs anti-terror laws, they must be the right ones. Unfortunately, many of the new laws suffer from serious problems, which is not surprising given that they run to hundreds of pages and have often been enacted and amended with great speed. To go from having no federal law to having a comprehensive regime in just a few years was always going to be difficult, especially when the new laws realign our legal system

through the extensive powers they grant to government and their impact on basic freedoms. The scope of the shift is unprecedented in Australian history.

In previous chapters we analysed the new laws and specific issues that arise under them. In this chapter we look at some of the big-picture, systemic problems that have emerged from the laws made over the last five years.

REACTIVE LAW-MAKING

Our response after September 11 has been essentially reactive, with each new bombing producing a new law – or often several new laws. By itself, though, a terrorist strike should not automatically mean that the government needs new powers. The need can only be determined by scrutinising our existing laws in light of what can be learnt from the attack.

Unfortunately, the new laws have been made with such haste that a careful assessment of where we already stand has been impossible. The laws passed after the London bombings in July 2005 were enacted so quickly that they came into force before two ongoing inquiries into the effectiveness of the existing laws could report. Before that attack, neither the government nor its key agencies were putting the case for an expansion of their powers, yet after the bombings the pressure proved irresistible.

As a result, laws were made without sufficient justification. Australia gained new laws, including laws dealing with preventative detention and control orders, yet the threat level to Australia as assessed by the government did not shift from "medium." Nor was new information made available to support such a major change in our law.

It is not surprising that our political leaders, as members of parliament and law-makers, have turned to new laws as a first response to terrorism. After each attack, the political pressures to act can be immense, and the political gains from being seen as "tough" on terrorism significant. At such a time, when in reality there may be little that Australian politicians can do about an

intractable international problem, new legislation is at least within their control and is a symbolic and potentially practical response.

We must be realistic about what new laws can achieve. There has always been and will always be a risk of a terrorist attack. If the goal is to eliminate that risk, we will fail. The law, no matter how stringent, cannot guarantee our security.

New laws cannot provide long-term solutions to terrorism. The legislation is unlikely to tackle its causes or deter a terrorist from a premeditated course of action. Law-making may even direct attention away from the debate over other, more effective, responses. As the drivers of change after a terrorist attack, feelings associated with grief, fear and political opportunity are some of the worst possible motivations. They are a poor justification for major legal change. Moreover, as history shows, the more repressive or draconian the law, the more likely it is that some people will take extreme action in response. In this way, the law might also become part of the problem.

The cycle of attacks followed by new laws is dangerous. Driven by fear and the need to act, we run the risk of a series of overreactions. This is the dynamic that terrorists rely on. What they cannot achieve by military might, they seek to achieve by stimulating our fears. By our own actions we may isolate and ostracise members of our community who, instead of assisting with intelligence-gathering, may then become susceptible targets for terrorist recruitment. Through our attempts to feel safe in the immediate term, we may actually make ourselves more vulnerable to terrorist attack.

POOR PROCESS

The law-making process got off to a bad start in 2002 when the first major counterterrorism Bill passed through the House of Representatives the same day it was introduced. Fortunately, the Senate then spent three months debating and amending it. As a result, the terror laws enacted during 2002 and 2003 demonstrate how Australian political institutions can play an important role in

achieving a balance between national security and human rights. Although some of the laws as enacted were quite stringent, the original Bills were far worse. We did not end up with the original legislation because it sparked a well-organised campaign led by community and legal groups and individuals. Their concerns fed into robust parliamentary inquiries, which examined the Bills and produced bipartisan reports recommending substantial changes. In many respects those recommendations were incorporated into the legislation.

Without that process, the outcome would have been far worse. As Prime Minister John Howard said on the first anniversary of the September 11 attack, "through the great parliamentary processes that this country has I believe that we have got the balance right."[33] Once he had control of the Senate, however, the Prime Minister sought to rush through new laws in response to the July 2005 bombings in London. His aim, he said, was to have the laws in place by Christmas – and that meant there was no time for an adequate Senate inquiry. Mr Howard announced the changes to the law on 8 September 2005 and the state and territory leaders endorsed them at a special meeting of the Council of Australian Governments on 27 September 2005.

With the Bills due in parliament in early November, there was very little time for public and parliamentary debate. But some extra notice of the contents of the Bill came when ACT Chief Minister Jon Stanhope posted a "Draft-in-Confidence" version of the law on his website on 14 October 2005, expressing concern about its impact on fundamental human rights. Mr Howard described the posting as irresponsible. The government also allowed more time for consideration after concerns were raised that parts of the law were unconstitutional. Nevertheless, the scrutiny process was still truncated.

The laws were duly passed by Christmas – in lightning fashion for legislation of such importance dealing with subjects as diverse as sedition and preventative detention of Australian citizens without charge. Remarkably, the compromise on the

sedition law involved an immediate inquiry by the Australian Law Reform Commission into whether it needed to be fixed. The decision to hold such an inquiry *after* the law had been put on the statute book – with a seven-year jail term as a penalty – is one of the more unfortunate illustrations of how our terror laws have been made.

Law-making in this style seems to have become habit. Another major law, passed in 2006, gave ASIO the power under the *Telecommunications (Interception and Access) Act 1979* to intercept the telecommunications of innocent people where this might, for example, "assist the Organisation in carrying out its function of obtaining intelligence relating to security." There was little public debate about the change, owing in part to the government's rushing the Bill through parliament. The Senate Legal and Constitutional Committee was given 26 days to conduct its inquiry and publish a report, giving interested people just twelve days to review and prepare a submission on a 90-page Bill that had taken the government six months to write. Unsurprisingly, the committee received only 24 public submissions, many from government agencies whose powers were to be increased, and held only one public hearing.

Despite the limited opportunity for public comment, the Coalition and Labor senators wrote a joint report recommending significant new safeguards. The Bill came on for debate in the Senate the day after the committee's report was tabled, giving senators no real time to read and digest its 65 pages. Two days later the Senate passed the law with only minor amendments, some of which did not come from the committee's report and may actually have made the Bill's flaws even worse.

The House of Representatives passed the Bill on the same day as the Senate made the amendments. All up, the government made sure that the Bill was passed within four days of the publication of the Senate committee report and that it incorporated virtually none of the recommended safeguards. Even the Attorney-General seemed to acknowledge that the Bill might not have struck the

right balance between security and protecting privacy. Just before the law was passed, he told parliament:

> The government will continue to consider in detail the committee report and the recommendations as part of its ongoing commitment to ensuring the regime achieves an appropriate balance. If there are further amendments that are thought to be appropriate following the consideration of the committee report, we will propose further amendments in the spring session of parliament.[34]

Instead of taking account of a bipartisan report and amending the Bill, the government passed the law anyway while saying that it might act later on the improvements suggested by the committee. This abridged, incomplete legislative process is another example of the worrying trend of enacting questionable anti-terror legislation in haste without proper scrutiny or debate. In a parliament where both houses are now controlled by the one side of politics, the checks and balances on the misuse of power and the passage of bad laws are too slight.

A LACK OF BALANCE

There must be a balance between our national security and fundamental freedoms. The object of new terror laws cannot be national security at all costs. They can only be justified to the extent that they protect our democratic freedoms and way of life. National security at the price of living in a totalitarian state is not something that Australians would accept.

Over the years many governments around the world, including in our own region, have sought new security powers only to use them against citizens or political opponents. As Sir Owen Dixon, a judge of the High Court of Australia, stated in 1951 in the *Communist Party Case*:

> History and not only ancient history, shows that in countries where democratic institutions have been unconstitutionally super-

> seded, it has been done not seldom by those holding the executive power. Forms of government may need protection from dangers likely to arise from within the institutions to be protected.[35]

This does not mean that our response to terrorism should be timid or that new laws are not warranted. It does, however, mean that the case for departing from accepted civil rights and key elements of our democracy must be fully justified and proportionate to the harm.

The question is how best to balance the security of the nation against the rights of its citizens. This task is made even more difficult when, after September 11, new laws have been made and old laws amended, often with great haste. Such change demonstrates how legal systems, and the basic principles that underlie them, like the rule of law and the liberty of the individual, can come under considerable strain in the aftermath of a terrorist attack.

In nations like Canada, New Zealand, the United Kingdom and the United States the answer is grounded in a domestic charter that protects such rights as freedom of speech, freedom of association and the right to a fair trial. Although the Australian Capital Territory has the *Human Rights Act 2004* and Victoria the *Charter of Human Rights and Responsibilities 2006*, Australia is now the only democratic country without such a national law. Our federal anti-terror laws are unique in the democratic world in being unconstrained by a charter that protects fundamental rights.

This is a problem because even though our political system has many strengths, it also has a key weakness. Parliament often does not work from an understanding of human rights principles, partly because, in the absence of an Australian charter, human rights can lack perceived legitimacy and political force. When they are needed most, they can be absent from the debate.

Charters of rights not only set out the fundamental rights of a nation's citizens, they also establish a way of weighing those rights against other competing demands such as national security. They remind governments and communities of a society's

basic values and of the principles that might otherwise be compromised at a time of grief and fear. After new laws have been made, a charter can also allow courts to assess the changes against human rights principles. This can provide a final check on laws that, with the benefit of hindsight, ought not to have been passed.

By contrast, the lack of an Australian domestic reference point on the basic rights attaching to citizenship means that we do not have effective mechanisms, judicial or otherwise, for determining whether rights have been unduly undermined by national security laws. There is occasionally a role for judges in this process, but this is usually at the margins of the debate, such as where constitutional provisions come into play or in interpreting laws.

As a result, if parliament is careful to avoid constitutional pitfalls and is express and unambiguous in its intent, it can abrogate a fundamental right. Even in the case of some of the early anti-terror laws, which were softened during a long and difficult parliamentary process, some measures go far beyond what can be justified. A five-year jail term for speaking about or reporting the detention of a person by ASIO, even where that person has been mistreated, is a striking example.

The lack of a legal check means that political and legal debate in the "war on terror" is largely unconstrained by fundamental human rights principles. Instead, the debate may reflect the majoritarian pressures of Australian political life rather than the principles and values on which the democratic system depends. The only check on the power of parliament or government to abrogate human rights depends on the quality of political debate and the goodwill of our political leaders. This is not a check that is regarded as sufficient in other nations.

•

It is natural that in response to terrorist bombings and graphic scenes of death and distress our fears will lead us to do all we can to protect ourselves and our families. One poll found that more than two-thirds of Australians believe that terrorists will strike

"before too long" and that a terrorist attack in this country is inevitable.[36] While such concerns naturally subside over time, each new attack somewhere in the world inevitably brings them back to the fore – along with pressure to enact a new wave of laws.

This is far from new. Writing in *The Federalist* in the late eighteenth century, US politician Alexander Hamilton observed:

> Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates. The violent destruction of life and property incident to war, the continual efforts and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they at length become willing to run the risk of being less free.[37]

What Australia needs at such a time are leaders who, rather than playing to our fears, help us to understand that we must accept a level of risk of terrorist attack, that there are limits to what the law can achieve and that the wrong laws can be costly. Practical measures such as increased airline and port security can make a real difference. On the other hand, if we strive for the illusory goal of full protection from terrorism using new laws, there is a danger that we will do even greater damage to our society and its freedoms and values than terrorism could ever achieve.

Five years since September 11, we risk reinforcing our legislative mistakes. Unfortunately, there is currently no sign that our law-makers will change course. New attacks will lead to new laws that will further erode our fundamental freedoms, increase fear and anger in parts of the community and make the problem more intractable. Indeed, it seems likely that we have seen only the beginning of the "war on terror." The laws we have today were unthinkable prior to September 11. It is equally hard to imagine the laws that we will end up with in the event of future attacks.

Endnotes

1. Dennis Richardson, "ASIO Today," AIAL Forum, April 2004, pp 25–26.

2. Mark Todd, "Chilling Warning: Terrorist Attack Is Feasible," *Sydney Morning Herald*, 14 October 2005, p 5.

3. Commonwealth of Australia, *Parliamentary Debates, House of Representatives*, 7 September 1939, p 164.

4. *Australian Communist Party v Commonwealth* (1951) 83 CLR 1.

5. The Criminal Code is a schedule to the *Criminal Code Act 1995.*

6. Commonwealth of Australia, *Parliamentary Debates, Senate*, 3 November 2005, p 43.

7. "PM's Wife 'Sorry' in Suicide Bomb Row," BBC News, 18 June 2002, <http://news.bbc.co.uk/2/hi/uk_news/politics/2051372.stm>.

8. *Report of the Security Legislation Review Committee*, Attorney-General's Department, Commonwealth of Australia, June 2006, p 162.

9. Australian Security Intelligence Organisation, "About ASIO: What is ASIO?," <www.asio.gov.au/About/comp.htm>.

10. *Attorney-General's Portfolio Budget Papers 2001–2002*, p 448; *Attorney-General's Portfolio Budget Statements 2006–2007*, p 210.

11. Australian Security Intelligence Organisation, "2004/05: The Year in Review," <www.asio.gov.au/Review/Contents/review/htm>; Commonwealth of Australia, Senate Legal and Constitutional Legislation Committee, Estimates hearings, 25 May 2006, p 54.

12. Commonwealth of Australia, Parliamentary Joint Committee on ASIO, ASIS and DSD, *ASIO's Questioning and Detention Powers: Review of the Operation, Effectiveness and Implications of Division 3 of Part III in the Australian Security Intelligence Organisation Act 1979*, November 2005, p 12.

13. Commonwealth of Australia, Parliamentary Joint Committee on ASIO, ASIS and DSD, *An Advisory Report on the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002*, May 2002, p vii.

14. Commonwealth of Australia, Parliamentary Joint Committee on ASIO, ASIS and DSD, *ASIO's Questioning and Detention Powers: Review of the Operation, Effectiveness and Implications of Division 3 of Part III in the Australian Security Intelligence Organisation Act 1979*, November 2005), pp 5–6.

15. *Immigration and Nationality Act of 1952*, section 236A (as amended by the *USA PATRIOT Act of 2001*).

16. T. Kelly, "Court Reveals FBI Deceit," *Sun Herald*, 25 August 2002.

17. Philip Ruddock, "Legal Framework and Assistance to Regions," Regional Ministerial Counter-Terrorism Conference, Bali, February 2004, paragraph 49.

18. *R v Kirby; Ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254.

19. *Grollo v Palmer* (1995) 184 CLR 348.

20. *Fardon v Attorney-General (Qld)* (2004) 210 ALR 50, 74.

21. *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

22. *A v Secretary of State for the Home Department* (2004) UKHL 56.

23. Lord Carlile of Berriew QC, *Report on the Operation in 2005 of the Terrorism Act 2000*, May 2006, paragraph 33.

24. UK *Terrorism Act 2006*, sections 1 and 2.

25. Australian Law Reform Commission, *Review of Sedition Laws*, Discussion Paper 71, May 2006, p 163.

26. Philip Ruddock, "Labor Continues Dishonest Campaign Despite Backflip on Sedition," Media Release 097/2006, 29 May 2006.

27. Phillip Boulten SC, "Counter-Terrorism Laws in Practice," paper presented at NSW Public Defender's Office Conference 2006, p 7.

28. Boulten, p 8.

29. Boulten, p 9.

30. *Lodhi v R* [2006] NSWCCA 121, paragraph 77.

31. *Lodhi v R* [2006] NSWCCA 121, paragraph 66.

32. Interview with Philip Ruddock, ABC Radio Hobart, 8 June 2006.

33. John Howard, speech delivered at the National Press Club, Canberra, 11 September 2002.

34. Commonwealth of Australia, *Parliamentary Debates, House of Representatives*, 30 March 2006, p 98.

35. *Australian Communist Party v Commonwealth* (1951) 83 CLR 1, 187.

36. Charles Miranda "Defiant in the Face of Terror," *Daily Telegraph*, 21 April 2004, p 1.

37. James Madison, Alexander Hamilton and John Jay, *The Federalist Papers*, Penguin Books, 1987, pp 114-15.

Australia's anti-terror laws are attracting renewed controversy as the legal system grapples with new crimes and the growing role of intelligence agencies. In just five years the Australian parliament has created 37 pieces of legislation dealing directly with terrorism – laws limiting freedom of speech and creating new categories of crime and new ways of dealing with suspects.

With so much change in such a short time it is difficult for Australians to judge the impact on their freedoms or to understand how the law works. In this book Andrew Lynch and George Williams provide a clear and accessible guide to the key components of Australia's anti-terrorism laws.

***What Price Security?* examines the new crimes of terrorism and the powers ASIO has to question and detain members of the community. It discusses sedition, control orders, preventative detention and how judicial processes have been modified to deal with terrorism offences.**

Andrew Lynch and George Williams have made major contributions to the public debate since September 11. In this book they examine whether Australia has gone too far in limiting democratic rights in the fight against terrorism.

UNSW PRESS

ISBN 0-86840-909-X

9 780868 409092

BRIEFINGS A series of short, topical books exploring social, political and cultural issues in contemporary Australia, published in association with Australian Policy Online, www.apo.org.au