THE HON MARK DREYFUS QC MP
Attorney-General
Minister for Emergency Management
Special Minister of State
Minister for the Public Service and Integrity

SPEECH

Protecting Australians under the rule of law

SECURITY IN GOVERNMENT CONFERENCE 2013

CANBERRA, TUESDAY 13 AUGUST

Introduction

I acknowledge the traditional owners of the land on which we meet – and pay my respects to their elders, past and present.

I also acknowledge Mr Roger Wilkins AO, Secretary of the Attorney-General's Department and Mr David Irvine AO, Director-General of Security, ASIO

It is a pleasure to join you for the 25th Security in Government Conference.

This is regarded as Australia's premier event on protective security, having become very well established since its first gathering in 1987.

Let me begin by reiterating that there is no greater responsibility for the Commonwealth than safeguarding the security of the nation and its people.

Despite advances in standards of living, technology and globalisation we live in a world where there are individuals and organisations that wish to do our nation harm, whether it is by violent physical attack, damaging our economy or by undermining our values. These threats arise particularly from those who seek to engage in terrorism, violent extremism and malicious cyber intrusions against our citizens and our nation.

The hard and sometimes dangerous work of the dedicated men and women who serve in our national security and law enforcement agencies is essential to protecting our nation and its citizens from these threats.

There have been many successes and good news stories about our successes in securing our nation's security, some of which I will touch on this morning.

But I want to begin by discussing some of the impacts and implications of the recent series of disclosures of classified information concerning the intelligence activities of the United States, one of Australia's closest allies.

These disclosures have given rise to concerns here about Australia's intelligence relationships with the United States and the United Kingdom, and more broadly, to concerns regarding how our intelligence agencies operate. Given the close relationship between the US and Australia, I am particularly concerned to ensure that those disclosures do not cause long-lasting harm to Australia's ability to identify and respond to the many threats that our nation faces.

Some people have suggested that all of the disclosures by Mr Snowden and Mr Manning were some kind of 'whistleblowing'. Where an activity has been authorised under law and overseen by appropriate Government bodies and where no wrongdoing has been identified, the disclosure of information is not 'whistleblowing'. This is a critical point that is often overlooked in much of the media coverage of the release of classified information by Mr Snowden in particular.

Many people within the Australian community have a strong and entirely legitimate interest in knowing that our intelligence

agencies are operating in a manner that is first, lawful, and secondly, that strikes a proper balance between respect for the privacy and other rights of individual citizens on the one hand, and the need to ensure that our agencies are able to gather sufficient intelligence to safeguard our national security on the other. While these two competing interests will exist in a state of tension in a democracy such as ours, giving rise to a legitimate and ongoing debate about where the balance should be struck, these interests are not contradictory.

Today is an appropriate opportunity for me to state that Australia's intelligence activities *are* carried out in a manner that is consistent with our laws, that these activities are subject to appropriate and rigorous oversight, and that the overarching purpose of these activities is to protect and reinforce Australia's democratic values.

National security, crime prevention and the need for intelligence gathering

Consistent with long standing practice, I am not going to discuss intelligence activities in detail, since to do so would potentially expose these important capabilities to those who would do us harm.

What I will say is that Australian intelligence agencies have made a significant contribution to our safety by constant and careful assessment of possible threats. This work saves lives at home and abroad. This includes the work of the Australian Security Intelligence Organisation for which I am responsible, as well as the work of the Australian Secret Intelligence Service, and the Australian Signals Directorate, among others.

At least four planned terrorist attacks designed to achieve mass casualties on Australian soil have been thwarted by agencies since 11 September 2001. Our intelligence work contributed to the arrest of over 20 terrorists.

Intercepted information has played an important role in recent counter-terrorism prosecutions and in preventing planned terrorist attacks.

In 2008, several men who faced trial in Melbourne were convicted of being members of a terrorist organisation. These men were known at the time as the Benbrika Group. The evidence that the Benbrika Group was engaged in preparing or fostering a terrorist act was largely contained in 482 conversations that had been intercepted by our intelligence agencies, authorised by appropriate warrants that were put before the jury at trial.

The collection of intelligence is not only essential to protecting our national security in the traditional sense that I have just

described. Intelligence gathering is also essential to protecting the Australian community from serious and organised crime.

The Australian Crime Commission's report *Organised Crime in Australia 2013*, released at the end of July, noted that the rapid development of technology, and the increasing availability of that technology throughout the world, has significantly increased the reach of organised crime.

The internet has become an integral part of daily life for most Australians, from online banking, shopping and social networking, to using email and browsing the web. Organised crime has seized on the opportunity to exploit for criminal gain the growing use of the internet by Australians, so much so that cyberspace now needs to be policed with a vigilance comparable to that exercised in our physical world.

Needless to say, this new frontier has created new challenges for our national security and law enforcement agencies.

The role of interception in protecting our nation and its citizens

It is imperative that our national security and law enforcement agencies have access to the right tools to carry out their functions. Telecommunications interception is one of the most effective means that Parliament has given our national security and law enforcement agencies to do their jobs. Although information

technologies have evolved rapidly, interception continues to be as relevant today as it was when the current legislation commenced in 1979.

To illustrate the importance of interception, in the 2011/12 financial year there were 5,928 prosecutions and 2,267 convictions based on lawfully intercepted material. Most of those were for serious criminal offences.

These figures may actually underestimate the effectiveness of interception because a conviction can be obtained without the intercepted material being used in evidence, even if it was very important to the investigation.

Interception also allows agencies to identify criminal connections, co-conspirators and organised crime associates, and assists in establishing the methodology of criminal enterprises. It also plays an important role in identifying those involved in using or spreading child exploitation material, and those involved in sexual slavery.

Safeguards

As I mentioned to at the outset of my remarks this morning, when talking about the challenges of securing the nation and its citizens it is important to also consider the issue of securing rights such as privacy.

This is not to suggest that privacy and security are in any way contradictory at a conceptual level. Both privacy and security are core values within our democratic society. We in Government have an obligation to protect the safety and security of Australians, and we also have an obligation to protect the privacy and freedoms of Australians.

This is because security is not an end in itself. Security is a condition that the state creates to enable its citizens to enjoy those rights and to live by the values that we hold dear.

For this fundamental reason, everything Australia does to combat terrorism, to combat violent extremism, to counter espionage and to promote and uphold a safe and peaceful country is carried out in accordance with the rule of law.

Everything our intelligence and law enforcement agencies do, is done to ensure that Australia remains a free, open and democratic society.

The legal and oversight arrangements of all Australian Government agencies should reassure all Australians that the privacy of their communications is appropriately protected.

It is entirely understandable that Australians want to know the answer to the question "who watches the watchers?". So I will now briefly explain some of the key legal arrangements that

ensure appropriate oversight of intelligence gathering by our national security and law enforcement agencies.

First, any access to communications in Australia must be in accordance with the provisions of the *Telecommunications (Interception and Access) Act 1979* and the *Telecommunications Act 1997*. It is the Interception Act that imposes a general prohibition on the unauthorised listening to or copying of communications in our country, while creating an exception to this rule that allows some Government agencies to lawfully access targeted communications provided that they obtain a warrant.

This means that telecommunications interception is only carried out under warrants issued by independent issuing authorities, including me as Attorney-General in the case of national security warrants. The use of interception is closely scrutinised through this system of warrants.

However, the answer to the question "who watches the watchers?" goes well beyond the warrant system under the Interception Act. There is a comprehensive network of oversight and integrity agencies. All of those agencies have access to the intercepted material, and some in turn have their own power to obtain interception warrants to investigate public malfeasance. I will speak about these bodies in more detail a little later.

Safeguards on intelligence agencies

The recent politically-motivated leaks of intelligence information have created an atmosphere of some scepticism towards intelligence agencies. I want to reiterate that Australia's intelligence activities are carried out in a manner that is consistent with our law, and for the purpose of protecting Australia's democratic values.

When working with our allies the sharing of information is simply a necessity. But I can assure you that there are strict limits on Australia's sharing of foreign intelligence with our allies.

The Australian Intelligence Community's intelligence gathering is governed by legislation including the *Intelligence Services Act 1997*, the *ASIO Act*, as well as the *Telecommunications (Interception and Access) Act 1979* and the *Telecommunications Act 1997* that I mentioned earlier.

It is important to be aware that there is a clear distinction between the work carried out by ASIO, and the work of our foreign intelligence agencies.

Intelligence Services Act agencies such as the Australian Secret Intelligence Service and the Australian Signals Directorate are required by law to obtain specific authorisation either from the

Minister for Defence or the Minister for Foreign Affairs to produce intelligence on an Australian.

There are limited grounds on which a foreign intelligence agency may seek a ministerial authorisation and those grounds are laid out specifically in the Intelligence Services Act. For example, the relevant Minister must be satisfied that the particular person is or is likely to be, a threat to security.

The legislation also places limits on retaining and disseminating information that has been collected on an Australian by one of our foreign intelligence agencies.

In this way we can allow the Australian intelligence community to acquire necessary foreign intelligence, while providing protections that limit the impact on privacy of their investigations.

All of our intelligence agencies are subject to independent oversight from more than one source. The Inspector-General of Intelligence and Security, with powers like those of a standing royal commission, reviews the activities of the Australian intelligence community to ensure that agencies act legally, with probity, that they comply with ministerial directives, and that they respect human rights.

In her most recent Annual Report, the Inspector-General concluded that overall she was satisfied that each agency within the Australian intelligence community understood and accepted its privacy obligations and had put appropriate measures in place to ensure that those obligations were met.

In addition to the general and significant oversight of the Inspector-General, all Australian Intelligence Community agencies are also subject to administrative oversight by the Parliamentary Joint Committee on Intelligence and Security, which takes seriously its obligation to hold all intelligence agencies to the highest standards.

The challenge of a changing security environment

Our law enforcement and security capabilities must keep ahead of the techniques and technologies employed by terrorists, agents of espionage and organised criminals who threaten our national security and the safety of our citizens. New technology requires our intelligence and law enforcement agencies to adapt to these changes and find new ways of gathering and locating information.

Protecting privacy in the context of the rapidly changing national security environment is a complex task. It requires us to constantly review and reassess privacy protection in the face of evolving technology. It requires us to recognize that our security and law enforcement agencies also play a direct and important

role in *protecting* privacy, as they combat identity theft, cyber-attacks and corporate espionage.

Protecting privacy also requires us to review and reassess the powers and tools available to our security and law enforcement agencies in response to changes in the threat environment and changes in community expectations.

Finally, it requires us to ensure that the oversight, accountability and transparency arrangements we have in place for our security and law enforcement agencies remain up-to-date and effective.

Our Government has not only built on the capability of our national security agencies, it has also developed the relevant legal framework. Over the past six years we have undertaken significant national security and privacy law reform. The Government continues to reform the law to get the balance right.

I have been struck by the silence of our political opponents on what they would do in the national security area if they got the chance. At the 2010 election the Opposition were virtually silent on national security issues. Their current policy pamphlet does have a section on counter-terrorism but it consists of only one sentence, which does not give us or the Australian public much to assess.

I assume from the virtual silence from the Opposition that they approve of the Government's current policy settings, and the resourcing of our national security agencies.

Achieving the appropriate legal framework in this area is complex. Let me briefly outline several of the major reforms that are now under consideration.

Review of the Telecommunications Interception Act

To begin the process of responding to the security and criminal threats posed by the changing technological environment, my predecessor Nicola Roxon referred a range of national security law reform issues to the Parliamentary Joint Committee on Intelligence and Security. The Committee held a number of public hearings and received more than 5,000 submissions from Government agencies, civil society, privacy advocates and ordinary members of the public.

The Committee tabled its report in Parliament in June of this year and has made a number of recommendations, which the Government will carefully consider.

One recommendation of particular relevance to my topic today was for a comprehensive rewrite of the Telecommunications Interception Act, so that the Act, which is now over thirty years old, can provide a clearer regime of protections and powers.

The Committee's recommendation that the Interception Act be comprehensively revised is welcome, and we will work with stakeholders to develop draft legislation for further consultation. Improving privacy protections, streamlining accountability and oversight requirements and clarifying industry obligations will be key areas of review.

Strengthening the Privacy Act

Our Government has also initiated a number reforms to improve the protection of privacy in our nation. The *Privacy Amendment (Enhancing Privacy Protections) Act* will come into force in March next year, significantly strengthening privacy protections for Australians by bringing Australia's privacy regime into the digital age.

These enhancements to privacy protection are intimately linked to information security. For example, the new Act puts extra obligations on companies that send personal information overseas to ensure that such information is protected to the same standard as if it were stored here in Australia.

Companies will have to develop detailed privacy policies – which must tell consumers how their personal information is to be handled, and how to make a complaint if their privacy is breached.

In addition, stricter rules will apply to the privacy of what is defined as "sensitive information", including health, DNA and biometric data.

The Commonwealth Privacy Commissioner will have the power to get an enforceable outcome – an apology, a retraction, a take-down notice or compensation – from a court. The Commissioner will be able to apply to the courts for a civil penalty order. For serious and repeated breaches of privacy, companies may be liable for more than a million dollars in penalties for unlawful privacy breaches.

Boosting Australia's National Security Capability

Finally, today I want to announce the delivery of a national security commitment that Labor pledged during the 2010 election campaign. Since that time agencies having been working on this detailed plan. I am very pleased to announce that the Government has delivered on its commitment to develop Australia's first *National Security Capability Plan*. This Plan:

- supports our unified approach to national security;
- complements the 2013 Defence White Paper; and
- supports the objectives and implementation of the National Security Strategy released earlier this year.

The Plan provides a comprehensive view of all the tools available to Government to understand the changing strategic environment. This is vital to assist with decision making – in both withstanding and responding to threats.

The Plan will allow agencies to better direct their collective capabilities – not only to adapt and respond to threats, but also to harness opportunities.

The Plan will be used to analyse our current capabilities and facilitate better, collective forward planning. This will then facilitate the identification of areas for collaboration and improved interoperability.

In conjunction with the Plan, we are also implementing a framework for our national security fusion capability. This will support greater collaboration and interoperability, which will assist agencies in adapting quickly to the changing threat environment.

As I am sure you appreciate – both the *National Security Capability Plan* and the framework to support our *National Security Fusion Capability* – are classified documents.

However, it is important to provide Australians with a better understanding of our national security arrangements. To that end

I am very pleased to launch the first *Guide to Australia's National Security Capability*.

This Guide provides an introduction to Australia's approach to national security and the capabilities that enable our agencies to achieve their critical objectives.

For the first time in one document, the Guide also describes the functions performed by the national security community, and the capabilities maintained by each agency.

It also includes a strategic statement of Australia's capabilities for each national security function, and highlights ways in which agencies are working towards the five year priorities identified in the National Security Strategy. I would like to take this opportunity to commend the efforts of the national security community in developing a more coordinated approach to meeting our national security challenges.

Conclusion

Protecting all of our citizens from threats to our national security and criminal activities is a complex and constantly changing task. It requires us to constantly review and reassess the effectiveness of the tools being used by our agencies to secure our nation, and at the same time to ensure the appropriate protection of the

privacy of our citizens in the face of evolving threats and our agencies' responses to those threats.

As I hope I have made clear this morning, the protection of privacy and the strengthening of accountability and oversight of the Australian intelligence community is an important objective, that our Government has delivered on. At the same time, our Government is working to ensure that our law enforcement and national security agencies are able to do their jobs effectively, investigating and prosecuting criminals and safeguarding the security of Australia in a changing threat environment.

The need to adapt to a changing threat environment also requires that the Government ensure that the oversight, accountability and transparency arrangements we have in place for our security and law enforcement agencies remain up-to-date and effective to their important functions.

I am confident that our Government has been able to deliver on these challenging and critically important policy objectives, and will continue to do so.

Thank you.