

1

Sachverständigengutachten gemäß § 29 PUAG

für den 1. Untersuchungsausschuss der 18. Wahlperiode, Prof. Dr. Patrick Sensburg, MdB (Vorsitzender)

von Prof. Dr. Stephan Bierling, Professur für Internationale Politik, Universität Regensburg

zum Thema

“Eingehende Darstellung der parlamentarischen, öffentlichen und wissenschaftlichen Debatte in Australien zu den Fragen der Tätigkeit der eigenen Nachrichtendienste, deren parlamentarischer Kontrolle und des Schutzes der Privatheit seit den Enthüllungen von Edward Snowden, einschließlich Zusammenstellung wesentlicher Dokumente, Erklärungen und sonstiger Veröffentlichungen von Regierung, Parlament, NGOs oder anderen Akteuren in diesem Bereich.”

Fertigstellung: 15. Juni 2015

Deutscher Bundestag
1. Untersuchungsausschuss
der 18. Wahlperiode

MAT A SV-9

zu A-Drs.: 72

Zusammenfassung der Ergebnisse:

Australien gehört mit den USA, Großbritannien, Kanada und Neuseeland zur Nachrichtendienst-Allianz „Five Eyes“ (FVEY). Im Zweiten Weltkrieg entstanden, ist sie die umfassendste bekannte Spionagekooperation der Geschichte. Die Snowden-Enthüllungen haben deshalb für Australien besondere Brisanz, treffen dort allerdings nur auf geringes Interesse und noch geringere Unterstützung.

Trotz der hohen medialen Aufmerksamkeit der Snowden-Enthüllungen betonten sowohl Premierminister Kevin Rudd (Labor, bis September 2013) als auch sein Nachfolger Tony Abbott (Liberal Party/in Koalition mit der National Party) ihre Politik des ‚no comment on intelligence matters‘. Davon abgesehen seien die Abhöraktivitäten der Vergangenheit stets rechtskonform gewesen. Die Sicherheit der australischen Bürger, aber auch die der Alliierten, so die Regierung, legitimiere den Informationsaustausch mit den Five Eyes-Partnern. Die Regierung spricht sich weiterhin für die enge Zusammenarbeit mit den Geheimdiensten der Five Eyes-Partner aus, insbesondere mit denen der USA. In der Abhör-Affäre um den indonesischen Präsidenten Yudhoyono hielt Abbott eine Entschuldigung für unnötig.

Im Parlament unterstützten die Abgeordneten der Labor Party und der Liberal Party/National Party den Kurs ihrer jeweiligen Premierminister. Beide Parteien sind gegen die Veröffentlichung von geheimen Dokumenten, Snowden ist für sie kein Held, sondern eine Gefahr für die nationale Sicherheit Australiens. Oppositionsführer Bill Shorten (Labor, seit September 2013) trägt die Linie der Regierung in Geheimdienstangelegenheiten in allen wesentlichen Fragen mit. Die Grünen sind die einzige Partei, die Regierung, Parlament und Geheimdiensten Versäumnisse vorwirft und Aufklärung und mehr Transparenz verlangt.

Aber die Debatte darüber wird seit Herbst 2014 von anderen Themen in den Hintergrund gedrängt: dem Aufkommen des Islamischen Staats und der Frage, was mit zurückkehrenden australischen Kämpfern geschehen soll, der Verhaftung von Männern in Sydney, Brisbane und Melbourne wegen Terrorismusverdachts, der Geiselnahme eines fanatischen muslimischen Einzeltäters in Sydney am 15. und 16. Dezember 2014 mit zwei Toten und den Anschlägen auf Charlie Hebdo in Paris am 7. Januar 2015. Ein Ende 2014 verabschiedetes Anti-Terror-Gesetz sieht vor, dass Bürger, darunter auch Journalisten und Whistleblower, die Details über Geheimdienstoperationen veröffentlichen, bis zu zehn Jahre ins Gefängnis kommen können. Ein weiteres Anti-

Terror-Gesetz, das im Frühjahr 2015 verabschiedet wurde, erlaubt den Geheimdiensten die Vorratsdatenspeicherung und ermöglicht die Aberkennung beziehungsweise Einschränkung von Bürgerrechten für Terrorverdächtige. Die Regierungskoalition und die oppositionelle Labor Party unterstützten diese Maßnahmen, die Grünen und einige unabhängige Abgeordnete waren dagegen.

Die Medien, allen voran die Qualitätszeitung „Sydney Morning Herald“, berichteten ausführlich über Snowdens Informationen und die Arbeit der Geheimdienste. In den Kommentaren kritisierten viele Journalisten insbesondere, dass australische und amerikanische Dienste den indonesischen Präsidenten und seinen Führungszirkel 2009 ausspionierten. Die Öffentlichkeit gab sich von den Enthüllungen hingegen weitgehend unbeeindruckt. Mitte 2014 hielten es 70 Prozent der Australier für „akzeptabel“, dass die Regierung Länder ausspäht, mit denen Australien keine guten Beziehungen hat. 50 Prozent akzeptierten dies sogar für Länder, zu denen Canberra gute Beziehungen hat. 62 Prozent der Australier hielten das Ausspähen von Indonesien für akzeptabel.

Insgesamt beschädigten die Snowden-Enthüllungen das Ansehen der australischen Geheimdienste kaum. Nur wenige NGOs oder INGOs protestierten gegen die Spionagepolitik der Regierung und die neuen Anti-Terror-Gesetze. Die Gruppe „Citizens Not Suspects“ etwa verurteilte die Regierungspläne zur Vorratsdatenspeicherung und wollte mit einer Petition den entsprechenden Gesetzentwurf „Telecommunications (Interception and Access) Amendment“ abschwächen. Das internationale „Committee to Protect Journalists“ kritisierte, dass es bei den neuen zehnjährigen Haftstrafen für Geheimnisverrat keine Ausnahme für Journalisten gibt. Eine wissenschaftliche Aufarbeitung der Snowden-Enthüllungen, der australischen Spionagepolitik und der neuen Sicherheits- und Anti-Terror-Gesetze fand bisher nur ansatzweise statt.

Inhaltsverzeichnis:

0. Zusammenfassung der Ergebnisse	2
1. Hintergrund	5
2. Regierung	9
3. Parlament	12
4. Medien	16
5. Öffentlichkeit	19
6. NGOs und INGOs	21
7. Wissenschaft	22
8. Verzeichnis der Quellen und Sekundärliteratur	23
9. Dokumente	24

Dank:

Bei der Recherche unterstützten mich meine Mitarbeiterin Anna Müller B.A., Angehörige des Stabs des *Parliamentary Joint Committee on Intelligence and Security* des australischen Parlaments sowie Dr. Dianne Heriot, die Leiterin der Parlamentsbibliothek in Canberra.

Biographie:

Dr. Stephan Bierling ist Professor für Internationale Politik an der Universität Regensburg. Seine Hauptforschungsgebiete sind die transatlantischen Beziehungen, die amerikanische Innen- und Außenpolitik und die deutsche Außenpolitik. Er nahm Gastprofessuren an renommierten Universitäten in den USA, Südafrika, Israel und Australien wahr. Bierling veröffentlichte mehr als vier Dutzend Aufsätze und zehn Monographien. Zuletzt erschien von ihm *Vormacht wider Willen. Deutsche Außenpolitik seit der Wiedervereinigung* (C.H. Beck 2014). Bierling kommentiert die internationale Politik in Zeitungen (u.a. SZ, FAZ, NZZ) sowie im Radio und im Fernsehen. 2013 wurde er in einem bundesweiten Wettbewerb der Zeitschrift UNICUM zum „Professor des Jahres“ im Bereich Geistes-, Sozial- und Kulturwissenschaften gewählt.

1. Hintergrund

Australien ist traditionell ein enger Verbündeter Großbritanniens, der USA, Kanadas und Neuseelands. Im Ersten und im Zweiten Weltkrieg kämpften diese Staaten gemeinsam gegen die Aggressoren in Europa und Asien. Australische Truppen unterstützten die USA im UN-mandatierten Koreakrieg und im Vietnamkrieg. Im Irakkrieg 1991, im Afghanistankrieg 2001 bis 2014 und im Irakkrieg 2003 bis 2011 war Australien Teil der von den USA geführten Koalitionen. Die USA hingegen verteidigten Australien im Zweiten Weltkrieg gegen japanische Angriffe und sind bis heute wichtigster Sicherheitsgarant des Landes. Diese enge Sicherheitspartnerschaft mit Washington drückt sich auch in der Tatsache aus, dass die USA ihre Militärpräsenz in Darwin (Northern Territory) bis 2017 auf bis zu 2500 US-Marineinfanteristen ausbauen werden. Für Australien stellt dies eine wichtige Rückversicherung in einer volatilen Weltregion dar, in der es keine multilateralen Sicherheitsorganisationen gibt. Auf der asiatischen Seite des Pazifischen Beckens bereitet der Aufstieg Chinas Sorgen, vor allem seine Ansprüche im ost- und südchinesischen Meer. Die in Australien amtierende konservative Koalition betont immer wieder die zentrale Rolle der USA als stabilisierende Kraft in Nordost- und Südostasien und die große Bedeutung der amerikanisch-australischen Kooperation.

Die geheimdienstliche Zusammenarbeit Australiens mit den USA, Großbritannien, Kanada und Neuseeland reicht ebenfalls in die Tage des Zweiten Weltkriegs zurück. Sie ist formalisiert im multilateralen *UKUSA Agreement* von 1946, besser bekannt unter dem Namen „Five Eyes“. Der Begriff „Five Eyes“ bezieht sich auf die Zahl der Teilnehmer an dem Abkommen und ein hohes geheimdienstliches Klassifizierungsniveau „(For your) Eyes Only“. Derart eingestufte Informationen werden nicht an außenstehende Regierungen, Ausländer oder internationale Organisationen weitergegeben. Australiens formaler Status als ein mit den USA und Großbritannien „zusammenarbeitendes Commonwealth-Land“ wurde im Jahr 1955 festgeschrieben. Die Five Eyes tauschen nachrichtendienstliche Informationen aus und spionieren sich nicht gegenseitig aus. Nach den Terrorattacken von 9/11 bauten die fünf Länder ihre elektronischen Überwachungsinstrumente stark aus und vertieften ihre Kooperation. Australien ist dabei insbesondere für das Abfangen und Speichern elektronischer Daten in Südasien zuständig.

Australien hat sechs Geheimdienste: 1) das *Office of National Assessments* (ONA), das die Auslandsspionage koordiniert und internationale politische, militärische und wirtschaftliche Ent-

wicklungen für den Premierminister und die Mitglieder des Nationalen *Sicherheitsausschusses* des Kabinetts analysiert; 2) die *Australian Security Intelligence Organization* (ASIO), die Informationen innerhalb Australiens sammelt, um die Regierung vor Sicherheitsbedrohungen zu warnen; 3) den *Australian Secret Intelligence Service* (ASIS), der Informationen über Fähigkeiten, Absichten und Aktivitäten von Personen oder Organisationen außerhalb des Landes sammelt und Spionageabwehr betreibt; 4) das *Australian Signals Directorate* (ASD), bis 2013 *Defence Signals Directorate* (DSD), das elektronische Nachrichten sammelt und analysiert und sich um die Sicherheit elektronischer Kommunikation kümmert; 5) die *Defence Imagery and Geospatial Organization* (DIGO), die raumbezogene und bildliche Informationen im Ausland sammelt und auswertet; und 6) die *Defence Intelligence Organisation* (DIA), die den Entscheidungsprozess der Regierung und der Streitkräfte in Fragen von Massenvernichtungswaffen, ausländischen Militärkapazitäten, transnationalem Terrorismus und Verteidigungsoperationen nachrichtendienstlich unterstützt.

Vor allem die Kompetenzen des Inlandsgeheimdienstes ASIO wurden seit den islamistischen Terroranschlägen auf das World Trade Center und das Pentagon am 11. September 2001, bei denen 11 Australier starben, auf Bali am 12. Oktober 2002, bei dem auch 88 australische Staatsbürger ums Leben kamen, und in London am 7. Juli 2005 massiv ausgeweitet. ASIO kann unter bestimmten Umständen Pässe einziehen, Computer und Computernetze ausspähen, die Kommunikation von verdächtigen Personen sowie von Personen überwachen, die mit einem Verdächtigen Kontakt haben, und Personen festsetzen, die Informationen über einen terroristischen Anschlag haben könnten. Diese Vollmachten gehen deutlich über diejenigen von Geheimdiensten vergleichbarer Länder wie der USA, Kanadas oder Großbritanniens hinaus. Die Reformempfehlungen des Unabhängigen Beobachters der Geheimdienste (Independent Monitor, von 2011 bis 2014 Bret Walker, seither Roger Gyles) und zweier Kommissionen zur Überprüfung der Arbeit der Dienste wurden von den jeweiligen Regierungen nicht aufgenommen. In seinem letzten Bericht kritisierte Walker Anfang 2014: „When there is no apparent response to recommendations that would increase powers and authority to counter terrorism, some skepticism may

start to take root about the political imperative to have the most effective and appropriate counter-terrorism laws.“¹

Die vom NSA-Mitarbeiter Edward Snowden gestohlenen und internationalen Medienvertretern übergebenen Dokumente belegen, dass die Five Eyes mehrere elektronische Überwachungsprogramme gemeinsam betreiben, darunter PRISM, XKeyscore, Tempora, MUSCULAR und STATEROOM. Bei PRISM, XKeyscore und STATEROOM arbeiteten der amerikanische Auslandsaufklärungsdienst National Security Agency (NSA) und das australische ASD eng zusammen. Die meisten der Snowden-Dokumente waren als „FVEY“ gekennzeichnet, durften also nur an die vier engsten Geheimdienstpartner der USA weitergegeben werden. Amerikanische und australische Nachrichtendienste unterhalten sogar eine gemeinsame Einrichtung für Aufklärungs- und Überwachungssatelliten mit dem Namen „Pine Gap“ bei Alice Springs in Zentralaustralien.² Laut einem Dokument aus dem Jahr 2006, das sich in den Snowden-Dokumenten fand, entwickelten die NSA und das ASD ein Programm, das dazu diente, über den „Zugang zu Computernetzwerken kryptografische Information und Material zu beschaffen“.³

Diese geheimdienstliche Zusammenarbeit wurde von konservativen Regierungen (John Howard/Liberal Party/1996-2007; Tony Abbott/Liberal Party/2013-) ebenso betrieben wie von sozialdemokratischen (Kevin Rudd/Labor Party/2007-2010 und 2013; Julia Gillard/Labor Party/2010-2013). Premierministerin Gillard verurteilte im November 2010 scharf die Veröffentlichung geheimer amerikanischer Dokumente auf der vom Australier Julian Assange gegründeten Internetplattform Wikileaks als „unverantwortlich und illegal“.⁴ Eine Untersuchung der Bundespolizei konnte aber keinen Rechtsverstoß von Wikileaks feststellen. Als die ersten Snowden-Enthüllungen im Juni 2013 publik wurden, übergab Premierministerin Gillard das Amt nach ihrer Niederlage in einem internen Machtkampf am 27. Juni 2013 gerade an ihren Vorgänger Kevin Rudd. Seit dem 18. September 2013 regiert Tony Abbott in einer Koalition seiner Liberalen Par-

¹ Independent National Security Monitor Annual Report 2014, 28.3.2014, 2.
<http://www.dpmc.gov.au/dpmc/publication/independent-national-security-legislation-monitor-annual-report-2014>
(6.5.2015)

² Philip Dorling: Australian outback station at forefront of US spying arsenal, Sydney Morning Herald, 26.7.2013.
<http://www.smh.com.au/it-pro/security-it/australian-outback-station-at-forefront-of-us-spying-arsenal-20130726-hv10h.html> (10.4.2015)

³ „Australien als bester Spionagefreund der USA“, Der Standard, 14.10.2014, 5.

⁴ Zit. in „Wikileaks acting illegally, says Gillard“, Sydney Morning Herald, 2.12.2010.
<http://www.smh.com.au/technology/technology-news/wikileaks-acting-illegally-says-gillard-20101202-18hb9.html>
(10.4.2015)

tei mit drei kleineren Parteien. Die Koalition verfügt im Repräsentantenhaus über 90 der 150 Sitze (Labor: 55, Grüne: 1, andere: 4), im Senat über 33 der 76 Sitze (Labor: 25, Grüne: 10, andere: 8).

Insgesamt befanden sich im Snowden-Material zwischen 15.000 und 20.000 Dokumente australischer Geheimdienste. Sie stammten zum Großteil vom ASD und konzentrierten sich auf die asiatisch-pazifische Region. Die für Australien heikelsten Enthüllungen aus dem Snowden-Material betrafen das Spionageprogramm gegen Indonesien. Im November 2013 veröffentlichten *The Guardian Australia* und die *Australian Broadcasting Corporation* (ABC) Belege dafür, dass das ASD 2009 versucht habe, die Mobiltelefone des indonesischen Präsidenten Ibu Ani Yudhoyono, seiner Frau und weiterer acht Mitglieder seines inneren Kreises während einiger Tage abzuhören. Auch habe sich das ASD 2007 zusammen mit der NSA während der Uno-Klimakonferenz in Bali 2007 bemüht, Telefonnummern indonesischer Sicherheitskräfte zu sammeln. Diese Enthüllungen führten zu einer deutlichen Abkühlung des Verhältnisses zu Indonesien, einem wichtigen politischen und wirtschaftlichen Partner Australiens. Jakarta berief seinen Botschafter aus Australien zurück, Malaysia bestellte den australischen Botschafter ins Außenministerium ein. Präsident Yudhoyono setzte die Zusammenarbeit im Verteidigungsbereich, beim Kampf gegen Menschenhändler und beim Austausch von Geheimdienstinformationen aus und forderte ein neues Verhaltensprotokoll.⁵ Nur langsam erholten sich die Beziehungen wieder.

Im Dezember 2013 berichtete *The Guardian*, das ASD habe bei einem Treffen mit Vertretern der NSA im Jahr 2008 angedeutet, Metadaten an die Partner-Geheimdienste weiterzugeben, selbst wenn australische Bürger betroffen seien.⁶ Allerdings stellte sich heraus, dass dies dem ASD nur dann möglich schien, wenn Daten eines australischen Bürgers im Ausland unabsichtlich abgefischt würden, und wenn ein Bürger ein unabsichtliches Ziel von Überwachung werde („as long

⁵ Vgl. Cameron Stewart/Paul Maley: Edward Snowden stole up to 20,000 Aussie files, *The Australian*, 5.12.2013. <http://www.theaustralian.com.au/national-affairs/foreign-affairs/edward-snowden-stole-up-to-20000-aussie-files/story-fn59nm2j-1226775491490> (27.4.2015)

⁶ Zit. bei Ewen MacAskill/James Ball/Katharine Murphy: Revealed: Australian spy agency offered to share data about ordinary citizens, *The Guardian*, 2.12.2013. <http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens> (10.4.2015)

as there is no intent to target an Australian national“).⁷ Im Mai 2014 veröffentlichte Glenn Greenwald, einer der drei Journalisten, denen Snowden die gestohlenen Geheimdienst Dokumente übergeben hatte, in seinem Buch *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* ein weiteres für Australien relevantes Dokument. In ihm bat der amtierende Stellvertretende Direktor des ASD die amerikanische NSA am 21. Februar 2011 um eine Verlängerung und Verschärfung der Überwachung der Kommunikation australischer Staatsbürger, die in Verbindung mit der Terrororganisation *Al Qaeda in the Arabian Peninsula* (AQAP) stehen: „We would very much welcome the opportunity to extend that partnership with NSA to cover the increasing number of Australians involved in international extremist activities – in particular Australians involved with AQAP.“⁸ Am 4. März 2015 kam heraus, dass sich das ASD zusammen mit Neuseelands *Government Communications Security Bureau* (GCSB) Zugang zu den Telefonnetzen Indonesiens und einiger kleiner Inselnationen im Pazifik verschafft hatte.⁹

2. Regierung

Die Regierung Rudd lehnte es mit Hinweis auf die bisherige Praxis ab, zu Geheimdienstangelegenheiten Stellung zu beziehen. Die Nachfolgeregierung Abbott behielt dies bei und betonte wiederholt, alle australischen Geheimdienste arbeiteten gemäß den Gesetzen, zu den Aktivitäten der Dienste werde sie sich nicht äußern.¹⁰ Als die Snowden-Dokumente die Abhöraktionen gegen Indonesien ans Licht brachten, lehnte Abbott im Parlament eine Entschuldigung dafür ab: „Australia should not be expected to apologise for the steps we take to protect our country now or in the past.“ Auch solle man von Australien nicht erwarten, „[to] detail what we do to protect

⁷ Zit. bei Christopher Joye: Did The Guardian get its latest spy story wrong?, *Financial Review*, 2.12.2013. <http://www.afr.com/news/politics/national/did-the-guardian-get-its-latest-spy-story-wrong-20131202-ij8mb> (5.4.2015)

⁸ Zit. in Glenn Greenwald: *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, New York 2014, 122. Siehe auch „Leaked Snowden documents reveal details of Australia’s bid for NSA help to spy on citizens“, *ABC News*, 15.5.2014. <http://www.abc.net.au/news/2014-05-14/documents-reveal-new-details-in-australias-bid-for-nsa-spy-help/5453764> (27.4.2015)

⁹ Vgl. Reissa Su: New Snowden Leaks Reveal Australia And New Zealand Spying On Indonesia, Pacific Island Nations, *International Business Times (Au Edition)*, 5.3.2015. <http://au.ibtimes.com/new-snowden-leaks-reveal-australia-new-zealand-spying-indonesia-pacific-island-nations-1426962> (8.4.2015)

¹⁰ Prime Minister Tony Abbott, Joint Doorstop Interview, Melbourne, 31.10.2013. <https://www.pm.gov.au/media/2013-10-31/joint-doorstop-interview-melbourne> (11.4.2015)

our country". Abbott versicherte weiter: „All our resources, including information“, seien genutzt worden, „ [to] help our friends and allies, not to harm them.“¹¹

In einem Interview im Januar 2014 bezeichnete Abbott Snowden als „Verräter“.¹² Außenministerin Julie Bishop warf Snowden in einer Rede in Washington, D.C. ebenfalls „schamlosen Betrug seiner Nation“ vor: „In June, a grave new challenge to our irreplaceable intelligence efforts arose from the actions of one Edward Snowden, who continues to shamefully betray his nation while skulking in Russia. This represents unprecedented treachery – he’s no hero. Snowden claims his actions were driven by a desire for transparency, but in fact they strike at the heart of the collaboration between those nations in world affairs that stand at the forefront of protecting human freedom. It was an attempt to destroy the trust between those who are most supportive of and sympathetic to the security and influence of the United States in maintaining global peace and freedom – Australia has not been spared.“¹³ Bishop betonte, die Zusammenarbeit der Geheimdienste sei eines der zentralen Elemente der australisch-amerikanischen Allianz im 21. Jahrhundert.¹⁴

Justizminister und Generalstaatsanwalt George Brandis war die Speerspitze der Regierung in der öffentlichen Auseinandersetzung mit den Snowden-Enthüllungen. Am 4. Dezember 2013 verurteilte er die Veröffentlichung der Geheimdokumente als schlimmsten Schlag für die westlichen Geheimdienste seit 1945: „The Snowden revelations are the most serious setback for Western intelligence since the Second World War and, given that most of the sophistication and the structure of Western intelligence-gathering was developed since the Second World War, it would not be an exaggeration to say it is the most serious ever. It is more serious than WikiLeaks, it is more serious than (Cold War British spies Kim) Philby and (Guy) Burgess and (Donald) Maclean, because of its extent. The extent of it is vast - we are talking about huge numbers

¹¹ Zit. in „Tony Abbott refuses to apologise for Indonesian spying program“, Sydney Morning Herald, 19.11.2013. <http://www.smh.com.au/federal-politics/political-news/tony-abbott-refuses-to-apologise-for-indonesian-spying-program-20131119-2xsn4.html> (10.4.2015)

¹² „Prime Minister Tony Abbott in Interview with Ray Hadley“, 29.1.2014. <http://www.pm.gov.au/media/2014-01-29/interview-ray-hadley-2gb-sydney> (10.4.2015)

¹³ Speech, Minister for Foreign Affairs, Julie Bishop MP, US-Australia: The Alliance in an Emerging Asia, Washington DC, 22.1.2014. http://csis.org/files/attachments/140123_FMBishop_Alliance21Speech.pdf (10.4.2015)

¹⁴ Vgl. Lisa Miller: Julie Bishop says intelligence gathering with US is vital, accuses Edward Snowden of treachery, 22.1.2014. <http://www.abc.net.au/news/2014-01-23/bishop-says-us-australia-intelligence-vital2c-accuses-snowden-/5214282> (27.4.2015)

of files which Snowden has put into the public domain.”¹⁵ Brandis betonte aber auch, die legislative und exekutive Kontrolle der Geheimdienste sei stark, im Parlament durch das *Joint Parliamentary Committee on Intelligence and Security* und das *Senate Select Committee on Defence and Foreign Affairs* sowie durch den *Inspector General of Intelligence and Security* auf Seite der Regierung.¹⁶

Einen Senator der Grünen, Scott Ludlam, bezichtigte Brandis wenig später der Sympathie für einen Verräter. Ludlam hatte in einem Meinungsbeitrag für *The Guardian Australia* am 14. Februar 2014 die Ausweitung der elektronischen Überwachung in Australien beklagt und eine vertiefte Debatte des Problems eingefordert.¹⁷ Brandis antwortete darauf im Parlament: „Senator Ludlam, you celebrate and make a hero of this man who, through his criminal dishonesty and his treachery to his country, has put lives, including Australian lives, at risk. I wonder how you can sit in this parliament and hold your head up high when you celebrate a man who, through criminal conduct and treachery, has put Australian lives at risk.”¹⁸ In einer Rede vor dem *Center for Strategic and International Studies* in Washington, DC im April 2014 ging Brandis noch einen Schritt weiter: Alle, die bezweifelten, dass Snowden ein Verräter sei, gehörten entweder zur „sich selbst-hassenden Linken“ oder zur „anarcho-libertären Rechten“.¹⁹ Weiter sagte Brandis: „I know some people naively claim that Snowden is a whistleblower. That claim is profoundly wrong. As *The Economist's* senior editor, Edward Lucas, points out in his recent book, *The Snowden operation*, Snowden meets none of the criteria of a whistleblower. According to a widely accepted series of tests developed by the Princeton scholar Professor Rahul Sagur in his book *Secrets and lies*, there are three principal criteria which define a whistleblower. First, a whistleblower must have clear and convincing evidence of abuse. Second, releasing the infor-

¹⁵ Zit. bei Cameron Stewart/Paul Maley: Edward Snowden stole up to 20,000 Aussie files, *The Australian*, 5.12.2013. <http://www.theaustralian.com.au/national-affairs/foreign-affairs/edward-snowden-stole-up-to-20000-aussie-files/story-fn59nm2j-1226775491490> (27.4.2015)

¹⁶ Zit. bei Renai LeMay: Snowden an 'American traitor', says Australia's Attorney General, *Delimiter*, 3.12.2013. <http://delimiter.com.au/2013/12/03/snowden-american-traitor-says-australias-attorney-general/> (27.4.2015)

¹⁷ Scott Ludlam: Internet surveillance: today is the day we fight back, 14.2.2014. <http://www.theguardian.com/commentisfree/2014/feb/11/day-fight-back-against-internet-surveillance-scott-ludlam> (20.4.2015)

¹⁸ Zit. bei Daniel Hirst: Scott Ludlam's support of Snowden 'celebrates treachery', says Brandis, *The Guardian Australia*, 12.2.2014. <http://www.theguardian.com/world/2014/feb/12/scott-ludlams-support-of-snowden-celebrates-treachery-says-brandis> (20.4.2015)

¹⁹ Zit. bei Nick O'Malley: Edward Snowden a traitor, Attorney-General George Brandis tells Washington Think Tank, *Sydney Morning Herald*, 9.4.2014. <http://www.smh.com.au/federal-politics/political-news/edward-snowden-a-traitor-attorneygeneral-george-brandis-tells-washington-think-tank-20140408-zqsqg.html> (19.4.2015)

mation must not pose a disproportionate threat to public safety. Third, the information leaked must be as limited in scope and scale as possible. Lucas concluded: 'Snowden has failed all three of these criteria'.²⁰ Im Juni 2014 betonte Premierminister Abbott bei einem Besuch in Kanada, dass die Arbeit der Five Eyes nicht nur zum Wohl der fünf Staaten sei, sondern auch „zum Wohl der ganzen Welt“. Schließlich leisteten „Amerika und seine Five Eyes-Verbündeten“ den Hauptbeitrag im Kampf gegen den internationalen Terror.²¹

Die australischen Geheimdienste selbst hüllten sich in der Frage der Snowden-Enthüllungen in Schweigen. Mit einer Ausnahme: Die *Australian Security Intelligence Organisation* (ASIO) – der einzige Geheimdienst des Landes, der einen jährlichen Tätigkeitsbericht vorlegt – schrieb in ihrem Bericht an das Parlament für das Finanzjahr 2013/14: „Edward Snowden is a compelling example of the wide-scale and indiscriminate harm that can be caused by malicious insiders. The damage caused by Snowden will be felt for many years. Of great concern is the very real potential the Snowden case will inspire and influence people who wrongly regard him as a whistleblower.“²²

Insgesamt verteidigte die Regierung Abbott konsequent die geheimdienstliche Zusammenarbeit der Five Eyes, bezeichnete Snowden als Verräter und kritisierte die Medien dafür, dass sie den Snowden-Enthüllungen zu große Aufmerksamkeit widmeten. Die Regierung weigerte sich auch, Informationen über die geheimdienstliche Arbeit preiszugeben oder überhaupt nur eine öffentliche Debatte darüber zu führen.

3. Parlament

Die oppositionelle Labor Party unterstützte den Kurs der seit September 2013 amtierenden konservativen Regierung weitgehend. Direkte Kritik gab es nie, allenfalls Verbesserungsvorschläge. So riet Oppositionsführer Bill Shorten dem Premierminister, einen konzilianteren Ton gegenüber Jakarta anzuschlagen. Er solle sich vielmehr wie US-Präsident Barack Obama verhalten, der

²⁰ Zit. in ASIO Report to Parliament 2013/14, 12.9.2014, S. 7. Kursivschreibung im Original. www.asio.gov.au/img/files/2013-14-Report_to_Parliament.pdf (19.4.2015) Vgl. Edward Lucas: Die Snowden-Operation. Eine folgenschwere Enthüllung. Veröffentlicht als Kindle Single im April 2014.

²¹ Prime Minister, Doorstop Interview, Ottawa, 8.6.2014. <https://www.pm.gov.au/media/2014-06-08/doorstop-interview-ottawa-canada> (10.4.2015)

²² ASIO Report to Parliament 2013/14, 12.9.2014, S. 7. www.asio.gov.au/img/files/2013-14-Report_to_Parliament.pdf (19.4.2015)

Kanzlerin Merkel nach Bekanntwerden der Abhöraffaire anrief und ihr versicherte, dass ihr Telefon gegenwärtig und künftig nicht abgehört werde. Der Abgeordnete Michael Danby, einer der wichtigsten Außen- und Sicherheitspolitiker der Labor-Fraktion, unterstützte die Verschärfung der Anti-Terrorgesetze und verurteilte Snowdens Enthüllungen.²³ Am 1. Dezember 2014 warf er Snowden und den Grünen vor, durch ihre Unterstützung der Veröffentlichung geheimen Materials die Sicherheit westlicher Zivilisten zu gefährden: „I have asked in this parliament a number of times why Mr Snowden and why the Greens support the release of material about how the Five Eyes, the Western intelligence services, intercepted telecommunications in northern Iraq prior to Daesh's conquering of that area. This is completely inimical to the safety of Western civilians.“²⁴

Die einzigen Abgeordneten, die Partei für Snowden ergriffen, kamen von den Grünen und Unabhängigen in Repräsentantenhaus und Senat. So lobte Senator Scott Ludlam (Grüne/Western Australia) Snowden im Juni 2013 als „Whistleblower, der der Welt einen Dienst erwiesen hat“.²⁵ Er kritisierte das Schweigen von Regierung und Labor Party zum PRISM-Skandal, „which, with some degree of success, I think, both of the old parties have managed to avoid treating as a scandal, as it is in every other world capital, by simply not making eye contact and pretending that it will all go away.“ Die Stellungnahmen der Regierung, so Ludlam weiter, seien 90 Prozent Plattitüden und zehn Prozent Informationen, die ohnehin schon bekannt sind.²⁶ Senator Nick Xenophon (Unabhängige/South Australia) wollte von der Regierung wissen, ob auch Parlamentarier überwacht worden seien, erhielt aber keine zufriedenstellende Antwort.²⁷

Senator Richard di Natale (Grüne/Victoria) pflichtete ihm am 4. Dezember 2013 bei. In anderen Nationen hätten Regierungschefs und Parlamentarier die US-Botschafter einbestellt, um Aufklä-

²³ Michael Danby: Speech, House of Representatives, 2.10.2014, 11235.
http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/2f675762-2571-4268-b435-28ce82b5e26c/0223/hansard_frag.pdf;fileType=application%2Fpdf (21.5.2015)

²⁴ Michael Danby: Speech, House of Representatives, 1.12.2014, 13711-13, hier 13713.
http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/2d891fab-c2b5-41b4-967f-0b37fdb6fe7c/0168/hansard_frag.pdf;fileType=application%2Fpdf (21.5.2015)

²⁵ Scott Ludlam: Speech, Senate, Speech, 19.6.2013, 3485-86, hier 3486.
http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansards/8bd37f80-48cf-484c-b5d6-09eeba7b9c15/0196/hansard_frag.pdf;fileType=application%2Fpdf (21.5.2015)

²⁶ Scott Ludlam, Rede im australischen Senat, 27.6.2013, S. 4294.
<http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansards%2F81320ab7-05a7-4deb-b6c9-aeba0e6b51bf%2F0177%22> (10.4.2015)

²⁷ Katherine Murphy: Australian government withheld knowledge of Prism program, The Guardian, 8.10.2013.
<http://www.theguardian.com/world/2013/oct/08/australian-government-knew-of-prism> (10.4.2015)

zung zu erhalten. Nicht so in seinem Land: „Here in Australia the response has been stony silence. We have seen almost a conspiracy of silence between the Labor Party and the Liberal Party on this issue.“ Alle Informationen verdanke man nur den Medien. Sie hätten getan, „what our own parliamentary oversight committee and other oversight bodies failed to do. [...]. It is also important to note here that our own parliamentary oversight committee has not yet been established for this parliament. So while that is being offered here as a justification for how these matters should be dealt with, we do not yet have a parliamentary oversight committee.“ Auch kritisierte di Natale, dass den Grünen Informationen durch den australischen Inlandsgeheimdienst ASIO verwehrt wurden, die der Oppositionsführer von der Labor Party erhalten habe: „Even the CIA and FBI do not enjoy the blanket protections that our intelligence agencies here enjoy.“²⁸

Angesichts der Tatsache, dass die überwältigende Zahl der Abgeordneten und Senatoren der Regierung oder der Labor Party angehört, verwundert es nicht, dass es keinen Untersuchungsausschuss zu den Snowden-Enthüllungen gab, und dass das *Joint Parliamentary Committee on Intelligence and Security* das Thema nur kurz aufgriff. Nach dem *Intelligence Services Act 2001* hätte es für eine Beschäftigung mit dem Thema durch den Ausschuss der Anweisung eines Ministers oder einer Entschließung eines der beiden Häuser des Parlaments bedurft. Das *Joint Parliamentary Committee on Intelligence and Security* hielt in seinem alle zwei Jahre erscheinenden Bericht lapidar fest: „The Committee also discussed with agencies the response of the AIC to disclosures by former National Security Agency contractor Edward Snowden.“²⁹

Am 12. Dezember 2013 gelang es den Grünen zumindest, im Senat, wo sie zu diesem Zeitpunkt mit neun Abgeordneten vertreten waren, mit Unterstützung der Labor Party eine Untersuchung („inquiry“) des elektronischen Überwachungsregimes in Australien zu initiieren. Die Untersuchung des Rechts- und Verfassungsausschusses des Senats erfolgte zwar primär deshalb, um frühere Berichte der *Australian Law Reform Commission* zur Privatsphäre („For Your Information“, 2008) und des parlamentarischen Geheimdienstsausschusses zur „Möglichen Reform der australischen Gesetzgebung zur Nationalen Sicherheit“ (Mai 2013) zu diskutieren und gesetzli-

²⁸ Richard di Natale: Rede im australischen Senat, 4.12.2013, S. 879.
http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansards/b37dd255-c7fa-4b2d-86de-64ef0517dde9/0135/hansard_frag.pdf;fileType=application%2Fpdf (12.4.2015)

²⁹ Joint Parliamentary Committee on Intelligence and Security: Review of Administration and Expenditure: No. 11 and No. 12 – Australian Intelligence Agencies, September 2014, S. 33.

che Schritte einzuleiten. Aber die Tatsache, dass die Untersuchung gerade zu diesem Zeitpunkt angesetzt wurde, war Folge von Snowdens Enthüllungen. Frühere Versuche, eine entsprechende Untersuchung zu lancieren, waren noch gescheitert. Vorsitzender des Ausschusses zur umfassenden Überprüfung des *Telecommunications (Interception and Access) Act 1979* wurde Senator Ludlam von den Grünen. Die anvisierten Fristen für den Abschlussbericht wurden mehrmals verschoben, auch weil es in dem Gremium durch Senatswahlen zu zahlreichen personellen Änderungen kam. Erst am 24. März 2015 konnte der Ausschuss seinen Bericht vorlegen.³⁰ Er beeinflusste die Diskussionen aber nur am Rande und hatte keinen Einfluss auf die Ausgestaltung des Gesetzes.

Zu diesem Zeitpunkt hatten Regierung und Labor-Opposition nämlich ihre Verschärfung der Anti-Terror-Gesetze gegen den Widerstand von grünen und unabhängigen Abgeordneten in drei Tranchen bereits vorangetrieben. Zunächst stimmten am 1. Oktober 2014 beide Häuser des Parlaments mit parteiübergreifender Unterstützung der *National Security Legislation Amendment Bill 2014* zu. Umstrittenster Punkt war Section 35P, die es zu einer Straftat mit bis zu zehn Jahren Gefängnis erklärte, Kenntnisse über Sonderoperationen der Geheimdienste (SIOs/Special Intelligence Operations) zu veröffentlichen. Darunter konnten potentiell auch Journalisten und Whistleblower fallen, wenn sie Informationen „grob fahrlässig“ („reckless“) publizierten. Generalstaatsanwalt Brandis versicherte jedoch, dass diese Klausel selten genutzt werden würde und die Arbeit der Medien nicht einschränke.³¹ Section 35P, so Brandis, ziele vor allem auf „Snowden-ähnliche Situationen“ ab.³² Er versicherte, dass Medienvertreter nur mit seiner persönlichen Genehmigung angeklagt würden. Allerdings dürfte die unklare Reichweite von Section 35P Zweifel bei Journalisten darüber wecken, ob sie eine Geschichte veröffentlichen sollen oder nicht.

³⁰ Comprehensive revision of the Telecommunications (Interception and Access) Act 1979, 24.3.2015. [http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal and Constitutional Affairs/Comprehensive_revision_of_TIA_Act/Report](http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act/Report) (20.4.2015)

³¹ Fact check: Journalists face 10 years' jail for exposing security agency bungalows, ABC News, 14.10.2014. <http://www.abc.net.au/news/2014-10-14/journalists-face-jail-for-exposing-security-agency-bungalows/5776504> (20.4.2015)

³² Daniel Hurst: George Brandis says laws would not catch journalists reporting Edward Snowden leaks, Guardian Australia, 4.11.2014. <http://www.theguardian.com/australia-news/2014/nov/04/george-brandis-laws-not-catch-journalists-edward-snowden-leaks> (20.4.2015)

Wenig später nahm das Parlament die *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* an, die Australiern die Ausreise untersagt, wenn sie sich Terrororganisationen anschließen wollen. Am 26. März 2015 verabschiedeten die Parlamentarier von Regierung und Labor-Opposition schließlich als dritten Teil der Anti-Terror-Gesetzgebung die *Telecommunications (Interception and Access) Bill 2015*.³³ Die Grünen und eine Mehrheit der unabhängigen Parlamentarier stimmten dagegen. Kern des Gesetzes war es, die Vorratsdatenspeicherung einzuführen und Internetdienste zu verpflichten, Metadaten zwei Jahre lang zu speichern. Um die Zustimmung der Labor Party zu erhalten, hatte die Regierung eingewilligt, den Zugang zu Quellen von Journalisten, die in Zusammenhang mit einer polizeilichen Untersuchung bei Geheimnisverrat stehen, nur nach einer richterlichen Anordnung zu erlauben. Auch revidierte die Regierung ihren gleich nach Amtsantritt gefällten Beschluss, das Gremium *Independent National Security Monitor* aufzulösen, das die Anti-Terrorismus- und Nationale Sicherheitsgesetzgebung überwacht.

Insgesamt vertraten Regierungskoalition und größte Oppositionspartei die gemeinsame Position, dass die Snowden-Enthüllungen die australische Sicherheit gefährdeten, und blockten weitere Auskünfte oder Untersuchungen ab. Nur die Parlamentarier der Grünen und einige unabhängige Abgeordnete verteidigten Snowden und kritisieren die von Regierung und Labor-Opposition beschlossene Vorratsdatenspeicherung. Aber ihre Versuche, die Regierung zur Herausgabe von Information zu drängen, blieben ebenso erfolglos wie ihr Widerstand gegen Gesetzesverschärfungen gegen Geheimnisverrat und für Vorratsdatenspeicherung.

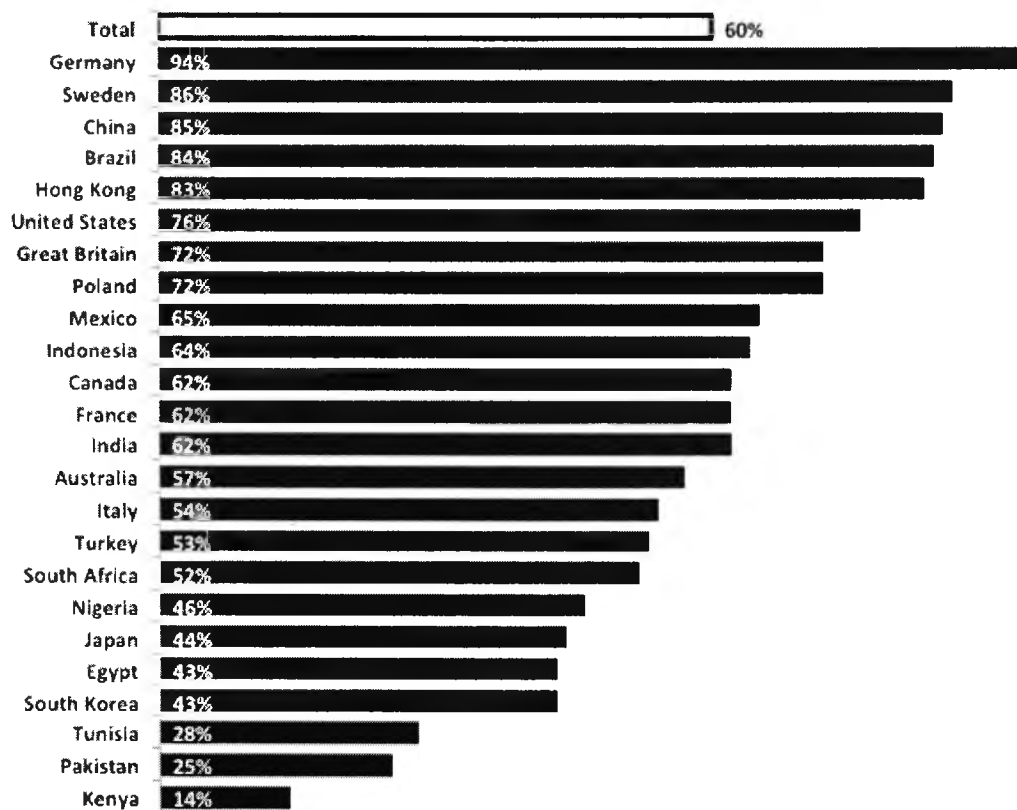
4. Öffentlichkeit

Die australischen Bürger interessieren sich weniger für die Snowden-Enthüllungen als die Bürger vieler anderer Nationen. Auch sind sie weniger bekümmert, was die Überwachung ihrer elektronischen Kommunikation durch ausländische Nachrichtendienste angeht. Das sind die beiden relevantesten Ergebnisse der Studie *Global Survey on Internet Security and Trust*, für die das

³³ Die parlamentarische Genese des Gesetzes und der Text finden sich unter http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r5375 (24.4.2015). Eine Kurzfassung bieten Jaan Murphy/Monica Biddington: *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, Bills Digest 89/2014-14, Department of Parliamentary Services, 26.3.2015, 88 S.

Centre for International Governance Innovation (Kanada) und das Marktforschungsunternehmen Ipsos (Frankreich) von 7. Oktober bis 12. November 2014 23.376 Personen in 24 Ländern befragten.³⁴ So hatten zum Beispiel nur 57 Prozent der Australier etwas von Edward Snowden gehört (Durchschnitt: 60%; Spitzenwert Deutschland: 94%).

Question: Have you heard anything about Edward Snowden, a US government contractor who leaked documents to the media showing that the US and other national governments have been secretly tapping into personal online accounts to collect information about people around the world?



Stichprobe: Alle Befragten (n=23.376)

Quelle: CIGI-Ipsos Global Survey on Internet Security and Trust

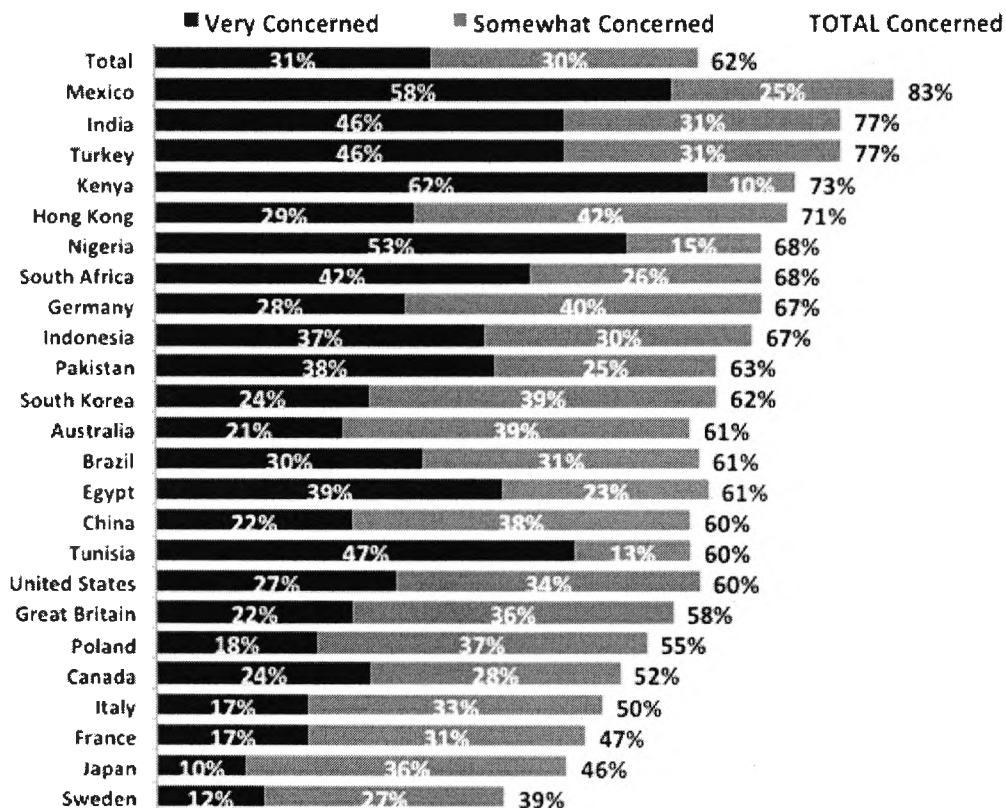
Auch sind die Australier mit 61 Prozent (Durchschnitt: 62%; Spitzenwert Mexiko: 83%) leicht unterdurchschnittlich besorgt, dass ihre Online-Aktivitäten von ausländischen Nachrichten-

³⁴ Centre for International Governance Innovation (CIGI)/Ipsos: Global Survey on Internet Security and Trust, 2014. <https://www.cigionline.org/internet-survey#survey-findings> (10.4.2015)

diensten im Geheimen ausgespäht werden. Nur 21 Prozent sind „sehr besorgt“ (Durchschnitt: 31%; Spitzenwert Kenia: 62%).

Question: How concerned are you about the following?

Government agencies FROM OTHER COUNTRIES secretly monitoring my online activities

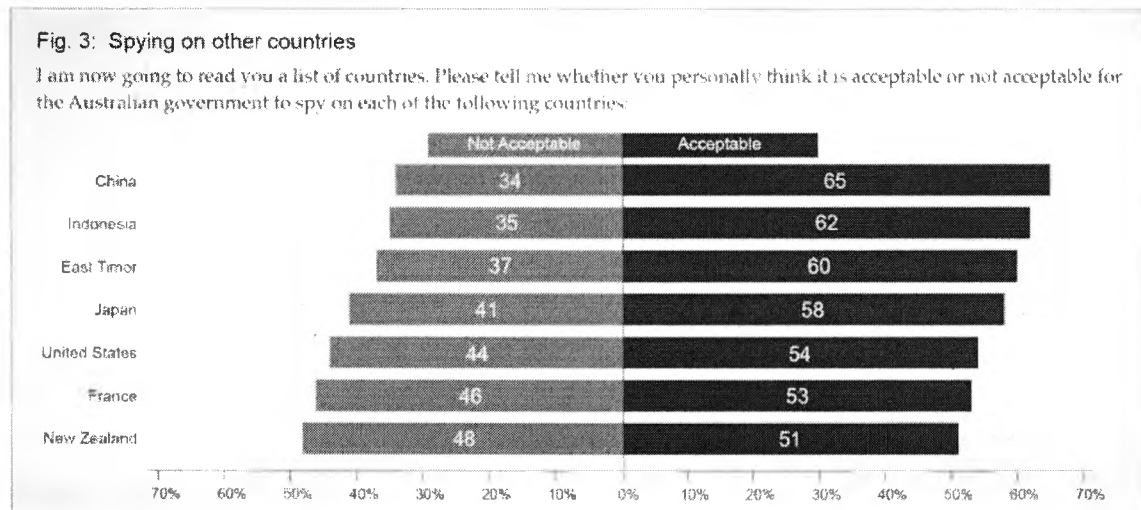


Stichprobe: Alle Befragten (n=23.376)

Quelle: CIGI-Ipsos Global Survey on Internet Security and Trust

Eine Umfrage des *Lowy Institute for International Policy* (Sydney) ermittelte, dass es 70 Prozent der Australier in Ordnung finden, wenn die australische Regierung Regierungen anderer Länder ausspioniert, mit denen sie keine guten Beziehungen pflegt. 50 Prozent der Australier halten Spionage sogar bei Ländern für akzeptabel, mit denen Canberra gute Beziehungen unterhält. Für 54 Prozent der Australier spricht nichts dagegen, wenn ihre Regierung ihren engen Bündnispartner USA ausspionierte.³⁵

³⁵ Lowy Institute for International Policy: The Lowy Institute Poll 2014, S. 6.
http://www.lowyinstitute.org/files/2014_lowy_institute_poll.pdf (10.4.2015)



Quelle: *Lowy Institute for International Policy*

63 Prozent der Australier sagten in einer repräsentativen Telefonumfrage des *Lowy Institute* zwischen 20. Februar und 8. März 2015, die neuen Gesetze zur Vorratsdatenspeicherung seien gerechtfertigt, um Terroranschläge zu verhindern und die nationale Sicherheit zu gewährleisten. Nur 33 Prozent hielten die Gesetze für ungerechtfertigt, weil sie zu sehr in die Privatsphäre der Bürger eingriffen.³⁶

Insgesamt gibt sich die australische Öffentlichkeit also mäßig interessiert an den Snowden-Enthüllungen, sieht keine allzu große Gefahr, von ausländischen Nachrichtendiensten ausspioniert zu werden und akzeptiert mehrheitlich das Ausspionieren anderer, selbst befreundeter Staaten. Die große Mehrheit der Australier glaubt, dass ihre Regierung ein akzeptables Gleichgewicht zwischen dem Schutz der Bürgerrechte und dem Kampf gegen den Terror gefunden hat.

5. Medien

Die australischen Medien berichteten intensiv über die Snowden-Enthüllungen und die Zusammenarbeit der australischen Geheimdienste im Rahmen der Five Eyes. Zwei der wichtigsten seriösen Tageszeitungen, *The Australian* (größte landesweite Zeitung, tägliche Auflage 2013;

³⁶ John Kerin: Poll shows support for data retention, *Financial Review*, 27.3.2015. Die Umfrage des Lowy Institutes wird im Juni 2015 veröffentlicht. <http://www.afr.com/news/politics/poll-shows-support-for-data-retention-20150327-1m9l10> (10.4.2015)

117.000, Wochenende: 255.000), die zum Medienimperium Rupert Murdochs – einem langjährigen Unterstützer Abbotts – gehört, und der *Sydney Morning Herald* (tägliche Auflage 2013: 132.000, Samstag: 228.000) nahmen sich des Themas immer wieder an. *The Guardian Australia*, eine 2013 gegründete Online-Zeitung (www.theguardian.com/au), trug als Teil der britischen *Guardian Media Group*, die exklusiven Zugang zu den Snowden-Dokumenten hatte, ebenfalls zur Information bei (monatlich 2 Millionen Leser). Auch die öffentlichen, großteils steuerfinanzierten TV-Stationen ABC und *Special Broadcasting Service One* (SBS One) berichteten regelmäßig über die Snowden-Enthüllungen, ABC war sogar führend an der Auswertung der Dokumente beteiligt. Während die Kommentare des *Sydney Morning Herald*, des *Guardian Australia* und von ABC die Spionageaktivitäten der Regierung in der Regel kritisierten, zeigten die des *Australian* mehr Verständnis für die Argumente der Regierung.

Angesichts der „No comment“-Politik der Regierung und der Zusammenarbeit von Regierungsfractionen und größter Oppositionsfraction im Parlament bei der Blockade jedweder Untersuchungen kam den Medien eine besondere Rolle zu, die Bevölkerung über die Ereignisse und Hintergründe zu informieren – oft zum Missfallen der Regierung. Premierminister Abbott warf dem staatlichen TV-Sender ABC sogar vor, eine politische Agenda zu verfolgen und Snowden eine Plattform zu bieten. In einem Interview sagte er: „Well, I was very worried and concerned a few months back when the ABC seemed to delight in broadcasting allegations by a traitor. This gentlemen Snowden, or this individual Snowden, who has betrayed his country and in the process has badly, badly damaged other countries that are friends of the United States and of course the ABC didn't just report what he said they took the lead in advertising what he said...“.³⁷ Der australische Premier musste sich allerdings wenig Sorgen machen: Die Bevölkerung war, wie oben geschildert, nur begrenzt empfänglich für die Informationen, die Snowden den internationalen Medien übergeben hatte.

³⁷ Prime Minister Tony Abbott in Interview with Ray Hadley, 29.1.2014. <http://www.pm.gov.au/media/2014-01-29/interview-ray-hadley-2gb-svdney> (10.4.2015)

6. NGOs und INGOs

Empört äußerten sich vor allem einige nationale und internationale Nichtregierungsorganisationen (NGOs und INGOs) über die Snowden-Enthüllungen, weil sie eine Beschränkung der Pressefreiheit und der Bürgerrechte fürchteten. Die australische Gruppe „Citizens Not Suspects“ verurteilte die Regierungspläne zur Vorratsdatenspeicherung und wollte mit einer Petition und Protesten den zur Debatte stehenden Gesetzentwurf *Telecommunications (Interception and Access) Amendment* abschwächen. Allerdings unterstützten nur 5897 Personen die Online-Kampagne, und die selbstgesetzte Marke von 10.000 Unterschriften wurde deutlich verfehlt.³⁸ Ein von drei Senatoren (Scott Ludlam/Grüne, Nick Xenophon/Unabhängige und David Leyonhjelm/Libertäre) organisiertes Protesttreffen im Parlament am 30. Oktober 2014 wurde von Vertretern der Kommunikationsindustrie und von NGOs besucht (*Communications Alliance, Australian Communications Consumer Action Network, Electronic Frontiers Australia, Pirate Party Australia, Blueprint for Free Speech, Civil Liberties Australia, Internet Society of Australia, Institute of Public Affairs, Australian Mobile Telecommunications Association, the Law Council of Australia, Liberty Victoria, the Media, Entertainment and Arts Alliance, the Australian Privacy Foundation, iiNet, the NSW Council for Civil Liberties* und *ThoughtWorks*).³⁹

Auch international fanden diese Proteste Unterstützung. Das in New York ansässige *Committee to Protect Journalists* äußerte in zwei „Alarmrufen“ („alerts“) am 17. Juli und 30. September 2014, es sei „tief besorgt“ über das neue Sicherheitsgesetz, das zu zehnjährigen Haftstrafen für Geheimnisverrat für Journalisten führen könnte. Ein zweites Anti-Terrorgesetz bestimmte, jeder Australier – also auch ein Journalist – müsse legitime Gründe angeben, um in bestimmte Konfliktgebiete zu reisen. Ansonsten sei dies ein kriminelles Vergehen. Der für Asien zuständige Programmkoordinator des *Committee to Protect Journalists*, Bob Dietz, sagte: „These bills would seriously hamper reporting in the public interest and we urge lawmakers to add the necessary safeguards to protect journalists and whistleblowers.“⁴⁰

Angesichts der geringen Empörung in Politik und Öffentlichkeit über die Snowden-Enthüllungen konnten die NGOs und INGOs allerdings kaum Einfluss auf die Debatte über die Tätigkeit der

³⁸ <https://www.getup.org.au/campaigns/privacy/mandatory-data-retention-efa--2/sign-the-petition> (10.5.2015)

³⁹ New South Wales Council for Civil Liberties, 30.10.2014.

http://www.nswccl.org.au/data_retention_secretcy_by_government_pussyfooting_by_labor (10.5.2015)

⁴⁰ *Committee to Protect Journalists: Australia's national security bills threaten press freedom*, 30.9.2014.

<https://cpj.org/2014/09/australias-national-security-bills-threaten-press-.php> (10.5.2015)

NSA und der eigenen Geheimdienste oder die neuen Sicherheitsgesetze entfalten. Auch die Zusammenarbeit mit den wenigen Parlamentariern, die sich gegen die übermächtige Regierung und die sie in dieser Frage unterstützende Labor Party stellten, blieb ohne nachvollziehbare Folgen.

7. Wissenschaft

Eine wissenschaftliche Aufarbeitung des NSA-Skandals hat bisher nicht stattgefunden. Fachzeitschriften blenden das Thema aus. Zu diesem Ergebnis führte die Überprüfung der Inhaltsverzeichnisse der relevanten Journale für den Zeitraum von Anfang 2013 bis Ende Mai 2015.⁴¹ Über die Anti-Terrorgesetzgebung informiert am besten das im März 2015 erschienene Buch von Andrew Lynch, Nicola McGarrity und George William: *Inside Australia's Anti-Terrorism Laws and Trials* (Sydney, 2015). Darin kritisieren die Autoren die Verschärfung der Anti-Terrorgesetze seit 9/11 als Überreaktion: „The result in Australia is a body of law that undermines democratic freedoms to a greater extent than the laws of other comparable nations, including nations facing a more severe terrorist threat.“ Und einige Zeilen weiter schreiben sie: „No other democratic nation has vested such an agency with a power like that which the Australian government has conferred upon ASIO.“⁴²

⁴¹ Ausgewertet wurden: *Australian Journal of International Affairs*, *Australian Journal of Political Science*, *The Australian Law Journal*, *Australian Quarterly*. Nur im *The Australian Journal of Politics and History* kommen die Snowden-Enthüllungen im halbjährlichen Jahresrückblick zur australischen Außenpolitik zur Sprache (Geoff Wade: Issues in Australian Foreign Policy January to June 2014, in: *The Australian Journal of Politics and History*, 60/4 2014; und Mark Beeson: Issues in Australian Foreign Policy July to December 2013, in: *The Australian Journal of Politics and History*, 60/2 2014). Im *Australian Journal of Public Administration* findet sich ein allgemein gehaltener Aufsatz über Whistleblowing im öffentlichen Sektor, jedoch ohne ersichtlichen Bezug zur NSA und zur eigenen Involvierung als Five Eyes-Partner, siehe dazu Marcia Miceli/Janet Near: An International Comparison of the Incidence of Public Sector Whistle-Blowing and the Prediction of Retaliation: Australia, Norway, and the US, in: *Australian Journal of Public Administration*, 72/4 2013.

⁴² Andrew Lynch/Nicola McGarrity/George William: *Inside Australia's Anti-Terrorism Laws and Trials*, Sydney 2015, positions 2686 und 2692 (Kindle edition).

8. Verzeichnis der Quellen und Sekundärliteratur

(Belege für Parlamentsreden von und Interviews mit Politikern sowie Zeitungsartikel und Beiträge von Online-Mediendiensten finden sich nur in den Fußnoten)

ASIO Report to Parliament 2013-14, 20.10.2014. <http://www.asio.gov.au/Publications/Report-to-Parliament/Report-to-Parliament.html>

Brandis, George: Securing Our Freedoms (speech delivered at the Center for Strategic and International Studies, Washington DC, 8.4.2014).
<http://www.attorneygeneral.gov.au/Speeches/Pages/2014/Second%20Quarter%202014/8April2014SecuringourFreedoms.aspx> (5.5.2015)

Centre for International Governance Innovation (CIGI)/Ipsos: Global Survey on Internet Security and Trust, 2014. <https://www.cigionline.org/internet-survey#survey-findings> (10.4.2015)

Comprehensive revision of the Telecommunications (Interception and Access) Act 1979, 24.3.2015.
http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act/Report (17.4.2015)

Greenwald, Glenn: No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, New York 2014.

Independent National Security Monitor Annual Report 2014, 28.3.2014.
<http://www.dpmc.gov.au/pmc/publication/independent-national-security-legislation-monitor-annual-report-2014> (6.5.2015)

Leslie, Tim/Corcoran, Mark: Explained: Australia's involvement with the NSA, the US spy agency at heart of global scandal, ABC News, 19.11.2013. <http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786> (20.4.2015)

Lynch, Andrew/McGarrity, Nicola/William, George: Inside Australia's Anti-Terrorism Laws and Trials, Sydney 2015.

Lowy Institute for International Policy: The Lowy Institute Poll 2014.
http://www.lowyinstitute.org/files/2014_lowy_institute_poll.pdf (10.4.2015)

9. Dokumente:

Angesichts der Blockadehaltung der Regierung und der Geheimdienste und des Fehlens einer parlamentarischen Untersuchung finden sich Stellungnahmen von Politikern zum Snowden-Material nur verstreut in Parlamentsreden, öffentlichen Auftritten und Interviews. Die wichtigsten sind im folgenden Anhang wiedergegeben. Zur Illustration der Medienberichterstattung und der Arbeit der NGOs sind einige Beispiele angefügt.

Dokumente in der Reihenfolge ihres Abdrucks

- 1) Scott Ludlam: Speech, Senate, Speech, 19.6.2013.
http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansards/8bd37f80-48cf-484c-b5d6-09eeba7b9c15/0196/hansard_frag.pdf;fileType=application%2Fpdf (21.5.2015)
- 2) Scott Ludlam, Rede im australischen Senat, 27.6.2013.
<http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansards%2F81320ab7-05a7-4deb-b6c9-aeba0e6b51bf%2F0177%22> (10.4.2015)
- 3) George Brandis: Securing Our Freedoms (speech delivered at the Center for Strategic and International Studies, Washington DC, 8.4.2014).
<http://www.attorneygeneral.gov.au/Speeches/Pages/2014/Second%20Quarter%202014/8April2014SecuringourFreedoms.aspx> (10.5.2015)
- 4) Michael Danby: Speech, House of Representatives, 1.12.2014.
http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/2d891fab-c2b5-41b4-967f-0b37fdb6fe7c/0168/hansard_frag.pdf;fileType=application%2Fpdf (21.5.2015)
- 5) Tim Leslie/Mark Corcoran: Explained: Australia's involvement with the NSA, the US spy agency at heart of global scandal, ABC News, 19.11.2013.
<http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786> (10.5.2015)
- 6) Ewen MacAskill/James Ball/Katahrine Murphy: Revealed: Australian spy agency offered to share data about ordinary citizens, The Guardian, 2.12.2013.
<http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens> (21.5.2015)
- 7) Ben Grubb: George Brandis in 'car crash' interview over controversial data retention regime, Sydney Morning Herald, 7.8.2014. <http://www.smh.com.au/digital-life/digital-life-news/george-brandis-in-car-crash-interview-over-controversial-data-retention-regime-20140806-101849.html> (10.5.2015)
- 8) Paul Farrell/Daniel Hurst: Journalists will face jail over spy leaks under new security laws, The Guardian, 16.7.2014. <http://www.theguardian.com/world/2014/jul/16/journalists-face-jail-leaks-security-laws> (10.5.2015)
- 9) Citizens Not Suspects: Online-Petition.
<https://www.getup.org.au/campaigns/privacy/mandatory-data-retention-efa--2/sign-the-petition> (10.5.2015)

Dokument 1:

THE SENATE
ADJOURNMENT

Whistleblowers

SPEECH

Wednesday, 19 June 2013

BY AUTHORITY OF THE SENATE

Wednesday, 19 June 2013 THE SENATE 3485

CHAMBER

SPEECH

Date Wednesday, 19 June 2013 Source Senate

Page 3485 Proof No

Questioner Responder

Speaker Ludlam, Sen Scott Question No.

Senator LUDLAM (Western Australia) (19:13): I rise tonight to make some remarks about whistleblowers, their importance to democracy and how their treatment reflects on the state of democracy in Australia and in other democracies around the world. I want to dedicate this contribution tonight to a great journalist, Mr Michael Hastings, who reported on whistleblowers and was one of the most genuinely courageous national security journalists working in the United States. I met him in London, in the northern winter, in December 2011. He and I, by coincidence, were on our way to the safe house where Julian Assange was being detained at the time. His death in a car accident in Los Angeles, at age 33, is a loss to all of us. May he rest in peace.

I have had something to do with whistleblowers in my time here. I have always been moved by their courage. The decision to blow the whistle has a profound effect on people's lives, and it can be an extremely lonely path. One person that comes immediately to mind for me is Dave Reid, a man who blew the whistle on the shocking state of health and safety standards and the culture at the radioisotope plant at the reactor complex in Sydney, at ANSTO. His revelations prompted inquiries and change, but he lost his job and he has paid a high price for his actions, even though official reports have vindicated his story and recommendation after recommendation have finally cleaned up some of the problems that he was pointing us to.

Thank you, Dave. You saw something, you did not turn away and you spoke up—and it cost you. The workers at ANSTO and the people of Sutherland shire are safer for what you did.

Private First Class Bradley Manning saw something, and he did not turn away either. He saw war crimes. He had evidence which showed deep and systematic wrongdoing. On 11 March this year we heard in his own words what his motivations were for blowing the whistle. He said in court that he hoped the release would:

... spark a domestic debate on the role of the military and our foreign policy in general as it related to Iraq and Afghanistan.

He also said:

I believed if the public was aware of the data, it would start a public debate of the wars.

Australia deployed troops in these wars. We are still complicit in them and their aftermath—one illegal war and one futile war.

Private Bradley Manning did spark a debate. He sparked a debate about whether killing journalists and children by remote control from helicopters is within the scope of international humanitarian law. He presented us all, the global community, with some brutal and haunting truths about how the laws of war and international human rights standards are violated in the ordinary course of conflict. For doing so, he was arrested and placed in an animal cage in Kuwait for months. He was kept naked for many more months with a light perpetually on, but he did not break.

Given what he has been through, the dignity of this extraordinary young man—he is 25 years old—is impressive and so is his statement to the court, which I now seek leave to table. This is the declassified statement of Private Bradley Manning to the court proceedings which are underway in the United States at the moment.

Leave granted.

Senator LUDLAM: After three years under harsh conditions, Private Bradley Manning is finally getting his day in court. He says:

The more I read the cables, the more I came to the conclusion that this type of information should become public. I agree with Bradley Manning, who has been incarcerated for three years.

I also thank the WikiLeaks publishing organisation, whose editor-in-chief has for one year this week been living in a room about the size of these two Senate wedges where I stand tonight. We learned much about our relationship

with the United States government and about our joint efforts with them—such as, for example, the efforts to weaken the treaty to ban cluster bombs. Citizens of this country, and of countries around the world, have the right to know what is being done in our names.

Professor John Keane, the author of *The Life and Death of Democracy*, talks about how vital the media and non-government organisations are to the health of democracy. He calls them the watchdogs, the guide dogs and the barking dogs of scrutiny. Such scrutiny is essential for holding institutions, governments and leaders accountable for their promises—to the standards that we agree and to the rule of law.

Somebody that I admire very much and had the opportunity to meet last January, Jacob Appelbaum, has described the price one pays for being a watchdog of democracy and for working to uphold human rights and for peace.

He said:

I don't have important conversations in the United States anymore. I don't have conversations in bed with my partner anymore. I don't trust any of my computers for anything at all. And in a sense, one thing that it has done is push me away from the work I've done around the world trying to help pro-democracy activists starting an Arab Spring, for example, because I present a threat, in some cases, to those people. And I have a duty as a human being, essentially, to not create a threat for people.

In the last week or two we have learned a new name, that of Edward Snowden. He has exposed the scale of

surveillance being undertaken by the United States National Security Agency. While some had suspected this and some had said it was probable, we now have a better idea about what nine corporations, Microsoft, Yahoo!, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple, said they did not know—that their servers were backdoored by the NSA to collect information on their customers, including us.

I am concerned now for the welfare of Edward Snowden, a whistleblower who has done the world a public service. I have put questions to this government on notice this week about whether our customs and immigration services have put a watch on this man to prevent him from entering Australia—as we know the British government have. He has stated that his greatest fear is that nothing changes as a result of his actions and his sacrifice. I found it extraordinary this week in this chamber to note the bipartisan blindfolding which seems to have occurred. Yesterday in this chamber we lost a vote—10 against the rest of the chamber—just to request the Attorney-General to make a public statement in the other place to inform Australians about the degree of our complicity. Perhaps Australia is not complicit. Perhaps we have not engaged in the systematic violations of the rule of law and customary democratic practice that we have seen in the United States. But we are owed that explanation by the Australian Attorney-General. Nobody in here yesterday would make eye contact as they voted that motion down. I will conclude by quoting a great philosopher, Robert Foster of Rap News. He said: Whistleblowers, they leak in the public interest, now what remains to be known is, is the public interested? If so, this might be a good day to exhibit it. Ignorance is choice in the age of the internet.

Quelle: Scott Ludlam: Speech, Senate, Speech, 19.6.2013.

http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansards/8bd37f80-48cf-484c-b5d6-09eeba7b9c15/0196/hansard_frag.pdf;fileType=application%2Fpdf (21.5.2015)

Dokument 2:

THE SENATE

MINISTERIAL STATEMENTS

Defence

SPEECH

Thursday, 27 June 2013

BY AUTHORITY OF THE SENATE

Thursday, 27 June 2013 THE SENATE 4294

CHAMBER

SPEECH

Date Thursday, 27 June 2013 Source Senate

Page 4294 Proof No

Questioner Responder

Speaker Ludlam, Sen Scott Question No.

Senator LUDLAM (Western Australia) (15:35): by leave—I move:

That the Senate take note of the document.

My motion is for the Senate to take note of the document Minister Jacinta Collins has presented on behalf of former Minister for Defence Smith. I acknowledge his comments in the other place, as he has chosen not to recontest at the next election.

This is a remarkably timed document from the former defence minister on our apparent full knowledge and concurrence about United States military and intelligence bases in this country. I say it is incredibly timed given that it comes in the wake of the PRISM scandal, which, with some degree of success, I think, both of the old parties have managed to avoid treating as a scandal, as it is in every other world capital, by simply not making eye contact and pretending that it will all go away. Of course, it will not, but nonetheless.

In this statement we have the Australian government declaring that it has full knowledge of what is going on in the United States bases on our territory. Several members of the United States congress and even a member of the homeland security committee have very recently expressed dismay that they had no idea how invasive and vast their own NSA surveillance activities are. How remarkable it is that Australian policymakers and the defence minister and staff have been brought into the loop that not even United States senior congressional representatives have been brought into.

Intelligence officials have told Fairfax reporters more in off-the-record statements about the PRISM system than parliamentarians have been able to extract from ministers in this place. We learnt, for example, that the new data centre under construction not too far from Canberra will be used to store material that has been extracted from PRISM by colleagues in the United States of the DSD and ASIO. We found that out in the Fairfax press because, when we put a motion up in here to have the Attorney-General make a statement to this parliament, both of the old parties refused to support it. Senator Xenophon and I have asked questions on and without notice, which

have been entirely fobbed off, about how much the Australian government knows about the massive surveillance overreach of citizens and whether the privacy of Australians has been breached. We know that it has. Do not treat us like children. We know what is occurring here. I think it would have been helpful for some transparency around the scope of the surveillance overreach, rather than just going into some kind of denial lockdown.

It is just as well that Fairfax journalist Phil Dorling is on the case, as there are so few good national security journalists in this country. There are a number, and Mr Dorling is certainly one of them. Without this small handful of people who track these issues closely, Australians would not know anything about how our government and intelligence officials have these huge volumes of immensely valuable information derived from PRISM and other US signals intelligence collection programs. The government says it has full knowledge and concurrence regarding US bases in Australia. Maybe that was intended to be comforting; I do not find it so. We are told in the statement around the basing of United States Marines in Darwin, an announcement that took the Australian people, and probably also the foreign minister at the time, completely by surprise. This is foreign policy conducted by press release after the key decisions have been made behind closed doors. Being presented with a decision after it has been made is not the same as full knowledge and concurrence, actually.

What knowledge do the Australian people or parliamentarians have about the rights, the roles and the responsibility of US forces while they are here on Australian soil? In November 2012, another Fairfax journalist at the time, Dylan Welch, who is now in Afghanistan, revealed that there was a secret two-page statement of principles relating to Australia and the US military collaboration. It is known as the Australia-United States Force Posture Review Working Group Statement of Principles. Mr Welch put in a freedom of information application about that process, and he was told that a letter from the defence department in the form of a statement of principles relating to Australian and US military collaboration existed. The DOD was obliged to consult with the US government, which, of course, told them not to release the document to Mr Welch. So the Australian people still do not have any knowledge of the underpinnings of a significant expansion of the US military presence into Australia.

The minister mentions North West Cape in his statement. That is in Western Australia. That is a facility that continues to facilitate, enable and support the passage and deployment of nuclear armed submarines. These are offensive attack weapons platforms. Ballistic missile submarines exist for no other purpose than Armageddon one day. They are not tactical weapons. They are not battlefield scale. They contain ballistic missiles with the intention of destroying cities and ending particular civilisations. That is what they are for. This base at North West Cape conducts communications with those vessels. Full knowledge and concurrence? Right.

Australia thereby legitimises the retention and deployment of nuclear weapons. Former and current Prime Minister—it is getting a little bit confusing—and former foreign minister Rudd worked quite hard as a middle power with a bit of diplomatic clout to bring forward the debate around nonproliferation and disarmament, through the commission that we co-chaired with the former foreign minister of Japan. At the same time as that process is trying to get consensus around nonproliferation and disarmament, we are writing into two successive defence white papers that we support the deployment of nuclear weapons in Australia's name. That is on paper.

On the ground, the existence of facilities like the North West Cape base are around enabling nuclear weapons deployment, not just in our name but on our soil.

Pine Gap, a nuclear weapons target and a key part of the US missile defence program, is, of course, a major incentive for other nuclear weapons states to keep their arsenals. We learn in the statement that that plays a great role in counterproliferation of nuclear weapons. Do not get me wrong: the extraordinarily sophisticated monitoring network that Australia supports is in our budget and is conducted with our international partners around detecting things like clandestine nuclear detonations, weapons tests and so on. I strongly support that, and we are told that the value of the data obtained on this issue from Pine Gap cannot be underestimated. So Pine Gap has somehow gone from being a secret intelligence facility to an anti-nuclear weapons establishment, which is remarkable. We are told that through this joint facility Australia is able to access intelligence. As we know, Pine Gap monitors radar, cell phones, radio and long-distance telecommunications, allowing it to provide targeting information for US air and ground forces, including drones and UAVs. It is extremely valuable because it is in the Southern Hemisphere. The Australian people do not know who the facility spies on or who is targeted. In 1999 the government refused to provide information about Pine Gap to this parliament's Joint Standing Committee on Treaties. Nothing has changed since then. Although US congressional officials have visited Pine Gap and received classified briefings about its functions, elected representatives and senators are entrusted with less information than can be found online or in a public library.

The Greens support the principle of this government providing statements of explanation such as this. The statement, however, is 90 per cent platitudes and 10 per cent information already in the public domain. Rather noticeably absent is the kind of material that a small handful of national security journalists are making available to the Australian people. It is time that the Australian government actually came clean so that the idea of full knowledge and concurrence does not become some sort of ironic afterthought once material is put into the public domain by a future generation of brave whistleblowers.

Quelle: Scott Ludlam, Rede im australischen Senat, 27.6.2013.

<http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22chamber%2Fhansards%2F81320ab7-05a7-4deb-b6c9-aeba0e6b51bf%2F0177%22> (10.4.2015)

Dokument 3:**Securing our Freedoms**

Speech by Attorney-General for Australia/Minister of the Arts, Senator the Hon George Brandis QC, to the Center for Strategic and International Studies

8 April 2014

Washington DC

May I begin by thanking the Centre for Strategic and International Studies for its hospitality in hosting this address? This is one of the world's most famous and influential centres for the study of international relations and the contemporary challenges of international politics. I am honoured to have the opportunity to speak at so illustrious a venue.

Today, I want to make some observations on the challenges facing democratic nations in protecting their populations from, and thwarting, those who would do us harm. I want to do so, in particular, from the perspective of the importance of information. For there can be no doubt, as all of you know, that there is no more important capability in thwarting terrorism than the collection of intelligence which can anticipate and stop terrorist events - whether Statesponsored; sponsored by non-State actors; or so-called lone wolf events.

Before passing on to my topic, however, let me begin by saying a few words about the relationship between my country Australia, and the United States of America. Yours is the country most Australians most admire. It is not an uncritical admiration, for the admiration of close friends never should be. But the majestic, untidy, inspiring, frustrating, show-stopping spectacle that is American democracy is one of the greatest achievements of mankind in the modern age.

As, in the months ahead, we pause to mark a baleful anniversary - the centenary of the commencement of the First World War - we should never forget that, in the course of that century, Australians and Americans fought side by side in every major war: the First World War, the Second World War (the Pacific War was directed, during its most perilous period, from General Macarthur's headquarters in my own home town, Brisbane; and Macarthur was quartered in a stately home only a couple of blocks from where I live); the Korean War; the Vietnam War; the Gulf War; the Iraq War; the Afghan War. Alone among the nations, Australians have fought beside you in every one of those conflicts. For more than 60 years, our security has been underwritten by one of your most longstanding treaties - the ANZUS alliance - invoked by the Australian government, for the first time, in the dark days after September 11 2001.

So Australians and Americans have much to be grateful to one another for: as brave comrades and as close friends. As you know, last year there was a change of government in Australia, and my party - the party of Robert Menzies and John Howard - was returned to government. But the view of the alliance, which I have expressed, is completely bipartisan. There could be no better proof of that than the presence here today of Australia's much-loved ambassador to the United

States, my friend Kim Beazley, who in his Parliamentary life led the other side of politics - the party of John Curtin and Bob Hawke - but today represents in Washington the whole of the Australian people on behalf of the new government of Prime Minister Tony Abbott.

I spoke just before of the great conflicts of the past century, in which our soldiers, sailors and airmen fought side by side and shed their blood for one another. In every one of those wars, our countries were reluctant participants. We fought to uphold the principles and values upon which our political systems are constructed and on which our societies are based: to defend them when we ourselves, or our allies, were attacked, and to extend them to the people of other lands.

Nobody has better captured those values than President Wilson, when he said in his speech to Congress on April 2 1917, seeking a Declaration of War against Germany:

"we shall fight for the things which we have always carried nearest our hearts - for democracy, for the right of those who submit to authority to have a voice in their own governments, for the rights and liberties of small nations, for a universal dominion of right by such a concert of free people as shall bring peace and safety to all nations and make the world itself at last free."

As is true of every generation, today the threats to freedom come from many sources. And, as nobody knows better than the people in this room, there is none more pervasive and insidious than terrorism. It has become commonplace to speak of the 'war' on terrorism - a metaphor much used, although not invented, by the second President Bush. And while there are important commonalities between terrorism and conventional forms of war, there are obvious differences as well. The most important, particularly in the age of the Internet, is invisibility. Terrorists marshal no armies. Their organizations are amorphous and mutable. Their warriors are lonely fanatics, not professional soldiers. And, for that very reason, the task of anticipating them is much more challenging.

Not that this is a new phenomenon. It was, after all, a single terrorist, Gavrilo Princip, who on June 28 a century ago precipitated the Great War in Europe when he assassinated the Archduke and Archduchess of Austria on a Sarajevo street. Margaret Macmillan, in her magnificent new study of the causes of the First World War - *The War That Ended Peace*, writes of the Young Bosnians and their terrorist organization, The Black Hand, as "mostly young Serb and Croat peasant boys who had left the countryside to study and work in the towns and cities. While they had put on suits in place of their traditional dress ... they nevertheless found much in the modern world bewildering and disturbing. It is not hard to compare them to the extreme groups among Islamic fundamentalists such as Al Qaeda a century later," Professor Macmillan writes. [pp. 513-4]

Of course, the Austro-Hungarian Empire had an extensive network of spies and informers. Its police kept the activities of The Black Hand under surveillance, and there is evidence that Princip was known to them. But they did not pick up his visit to Sarajevo that fateful Sunday.

Now, as then, information is the key. The difference between the world on the eve of the Great War, and the world of today, is that there is so much more information, and so much more communication. Terrorists no longer plan their crimes over hushed conversations in coffee shops (although no doubt some still do). The sheer volume of information, and the internationalization of terrorist networks mediated through modern telecommunications, poses huge challenges for na-

tional security agencies, in terms of resourcing alone. But intercepting and correctly analysing that traffic is at the heart of the global counterterrorism response.

Yet, as we are all well aware from the heated public debate in both of our countries, following the Snowden revelations, the question of the extent to which the state should invade the privacy of its citizens by the collection of intelligence will always be a controversial one. Some, usually those with a better informed appreciation of the capabilities and danger of sophisticated modern terrorism, would wish for fewer limitations on intelligence gathering, in the name of public safety. Others, most commonly those who do not bear responsibility for the protection of the public and who have the luxury of approaching the question from a largely philosophical or legalistic perspective, argue that there should be much wider limitations upon the collection of intelligence. However there are few - very few - who take the absolutist position that either there should be no collection of intelligence, or alternatively no limitations on its collection.

The governments of both of our countries have struggled with this issue in recent months. By the way, it is only liberal-democratic states which *would* struggle with the issue at all: in the authoritarian systems which beget the terrorism from which we seek to defend our selves, there would be no such argument. But, as Aharon Barak, the former President of the Supreme Court of Israel, famously remarked in 2005, democracies fight terrorism with one arm tied behind their backs.

Australia has closely watched the evolution of this debate in the United States, and I have studied with care, and during my visit to Washington had many conversations about President Obama's Presidential Policy Directive of 17 January. Australia welcomes the President's clarification of American intelligence collection policies embodied in that directive. That is not to say, of course, that Australia would necessarily have resolved these policy choices in the exactly the same way. Every country's needs and circumstances are peculiar to it.

In the post-Snowden environment, one thing which remains just as critical as it has ever been - indeed, even more critical - is that longstanding allies remain committed to their close cooperation in intelligence-gathering and intelligence-sharing. Along with our friends in the United Kingdom, Canada and New Zealand, Australia and the United States are part of the quintet of Western democratic nations which have for many years collaborated intimately in such matters. That collaboration must continue unaffected by the Snowden fall-out and I am confident that it will.

I am not, in the course of these remarks, going to attempt to tackle the deep ethical and legal issues at stake concerning intelligence-gathering, let alone to comment on domestic American politics. As a lawyer, I have a bred-in-the-bone respect for due process and civil liberties. But I must confess frankly that, as the minister within the Australian system with responsibility for homeland security, the more intelligence I read, the more conservative I become. The more deeply I come to comprehend the capacity of terrorists to evade surveillance, the more I want to be assured that where our agencies are constrained, the threat to civil liberty is real and not merely theoretical.

I turn, then, to address some of the policy issues which confront us in the collection and use of intelligence in the cause of defending our populations from terrorism. Those issues all point to the critical importance of Australia and the United States continuing to act as close and collaborative partners, as we always have done in the past.

The events of September 11, 2001 reshaped the counter terrorism landscape. Amongst the many people who lost their lives that day were 10 Australians. While this pales in comparison to the number of American casualties, it demonstrates that this was an attack on Australia as well – as it was on the dozens of other nations whose citizens were murdered that day. Its effect was to profoundly challenge our own national security philosophies.

By a bizarre coincidence, the then Australian Prime Minister John Howard was in Washington on 9/11, to commemorate the 50th anniversary of the ANZUS Treaty, the bedrock of our alliance which had been negotiated between the Truman Administration and the Menzies Government half a century before. Three days later, in response to the September 11 attacks, the Australian Cabinet invoked Article IV of the ANZUS Treaty for the first time, signalling Australia's intention to support the US in efforts to bring those responsible to justice. In doing so, Prime Minister Howard declared the terrorist strikes to be an attack not only on the US, but on Australia and indeed against other Western nations in general.

Barely a month later, on 17 October 2001, 10 days after the US announced the commencement of "Operation Enduring Freedom" against Taliban Forces in Afghanistan, Prime Minister Howard committed 1550 Australian military personnel to assist in the international effort. Our partnership in Afghanistan and Iraq resulted in a new level of collaboration between Australia and the United States. In a July 2003 report, the Australian Strategic Policy Institute (ASPI) noted:

"...the events of September 11 mark a fundamental turning point in the dynamics of the US-Australia relationship, with a much strengthened trend to an even deeper and closer alliance than before."

Over the decade or more since 9/11, some commentators began to suggest that terrorism no longer posed as significant a threat to national security as it once did. That view is simplistic and frankly wrong. While there is some evidence that we are witnessing a shift in terrorism tactics and techniques from large-scale, September 11 style attacks to 'lone-actor', smaller-scale, multi-mode attacks, a change of terrorist tactics if that is what is occurring, is not equivalent to a diminution of the terrorist threat.

In fact, such a shift in tactics creates significant new difficulties for law enforcement and intelligence agencies in identifying 'lone-wolves' who, due to their autonomous activities, are less likely to attract the attention of law enforcement and security agencies during the planning phases of their operations. Such tactics were vividly demonstrated in Boston as well as in the United Kingdom last year.

Countries must continue to work together against the global terror threat wherever it is originating, and not simply view threats and vulnerabilities as local versus international. There is much evidence to suggest that so called home-grown or regional threats are influenced, if not directly assisted, by offshore events and groups.

More than any other recent conflict, Syria - and the terrorist activity and training that are taking place behind the fog of the Syrian civil war - highlight not only that the global threat of terrorism remains undiminished, but that it will continue to evolve and leave a range of legacy issues over the short to medium term. Terrorists will continue to adapt and look to new technologies and changing, volatile global situations.

As terrorist tactics and operational doctrine evolve, security agencies must develop and maintain effective capabilities in order to mitigate the ongoing threat.

I am sorry to have to tell you that per capita, Australia is one of the largest sources of foreign war fighters to the Syrian conflict from countries outside the region. On 3 December 2013, two Sydney men were arrested and charged with foreign incursion-related offences as part of a Joint Counter Terrorism Team investigation carried out by Australian police and Australian authorities who continue to monitor recruitment, facilitation and financing of terrorist activity in Syria from Australian sources.

We also know that Australians are taking up senior leadership roles in the conflict. This shows that as a nation we need to address this issue early, in order to prevent individuals from travelling to participate in that and other foreign conflicts. This is, of course, not a new concern for Australia, nor other countries. Between 1990 and 2010, the Australian Government investigated at least 30 Australians who travelled to conflict areas such as Pakistan and Afghanistan to train or fight with extremists. 19 engaged in activities of security concern in Australia upon their return, and eight were convicted in Australia of terrorism-related offences and sentenced to up to 28 years in prison.

While not new, the difference is the scale of the problem. The number of Australians participating in the conflict in Syria is higher than we've experienced with previous conflicts, with assessments of between 120 and 150 Australians travelling to the greater Syria region to participate in the conflict. In mid-2013, the conflict reached a new milestone as the number of foreign fighters exceeded that of any other Muslim conflict in modern history.

The Australian Government is currently considering a number of measures to discourage and deter Australians from travelling to Syria to participate in the Syrian civil war and undertake training. These measures broadly come under four headings:

1. **Disruption**—stopping individuals from travelling or facilitating the travel of others or otherwise providing support to the conflict;
2. **Response**—responding to individuals who have travelled to Syria;
3. **Risk management**—managing the risk of those who have been prevented from travelling, or those who have travelled and returned; and
4. **Prevention**—reducing the pool of those who might seek to travel or participate in the conflict.

I cannot stress enough that international engagement, intelligence collection and information sharing will continue to be vital to this effort.

The Syrian civil war is significant, not only because Syria has now become one of the most important centres of terrorist activity, but also because it reminds us of the pervasiveness, mobility and ambition of modern Islamist terrorism. It is yet another reminder to the democratic world of the intractability of the terrorist threat. This problem will not just go away and peaceful nations must never become complacent or lower their guard against the threat that terrorism poses. They must remain vigilant, committed and cooperative in their joint efforts to defeat it.

What does this mean for our future? Forecasting is an attempt to predict tomorrow from the ripples of the past and the events of the present. But the direction of history is never lineal, and it is

often random, unpredictable events which change the course of history. Think of June 28 1914 in Sarajevo, or indeed September 11 2001 in New York and Washington. Some people call these events 'black swans'. While we justify their occurrence in hindsight, they profoundly change our calculations of risk. 'Unknown unknowns,' as Donald Rumsfeld might have said.

I believe that Australia and the United States are better placed than at any time to respond to hostile events both predictable and random. Experience from events like September 11 means that our national security structures are more agile, our information sharing mechanisms are more sophisticated and our policy is focused on building resilience and implementing prevention strategies instead of just responding to singular threats or mere responding to events after they have taken place.

We need to ensure our arrangements, capabilities, legislation and relationships are significantly well developed and maintained to enable us to deal with our future national security environment defined by both identified risks and unidentified contingencies.

The dangers which I have described are the principle reason why the compromise of our intelligence by Edward Snowden was so profoundly damaging to the interests of both of our countries. The massive damage which Snowden's disclosures caused was at two levels. Obviously, the revelation of intelligence content was hugely damaging to our interests. But no less concerning – indeed, arguably even more damaging – was what those disclosures potentially revealed about our capability. The problem of 'going dark' has been raised in recent years. 'Going dark' refers not to the absence of legal authority to conduct interception, but the practical difficulties in obtaining information.

People who pose national security threats are using disclosed information to update their methods and avoid detection by our agencies. Criminals similarly use the information to avoid detection and prosecution. Capability, which can be decades in development and expect to enjoy a significant operational life expectancy, may be potentially lost over night. Replacing capability after a set-back is not a fast process and attracts substantial cost. The harms of the Snowden disclosures will continue to be felt for an unpredictable time to come.

I know some people naively claim that Snowden is a whistleblower. That claim is profoundly wrong. As *The Economist's* senior editor Edward Lucas points out in his recent book *The Snowden Operation*, Snowden meets none of the criteria of a whistleblower. According to a widely-accepted series of tests developed by the Princeton scholar Professor Rahul Sagar, in his book *Secrets and Lies*, there are three principal criteria which define a whistleblower.

First, a whistleblower must have clear and convincing evidence of abuse.

Second, releasing the information must not pose a disproportionate threat to public safety.

Third, the information leaked must be as limited in scope and scale as possible.

Lucas concluded: "*Snowden has failed all three of these criteria*". I agree.

Snowden is not a genuine whistleblower. Nor, despite the best efforts of some of the gullible self-loathing Left, or the anarcho-libertarian Right, to romanticize him, is he any kind of folk hero. He

is a traitor. He is a traitor because, by a cold-blooded and calculated act, he attacked your country by significantly damaging its capacity to defend itself from its enemies, and in doing so, he put your citizen's lives at risk. And, in the course of doing so, he also compromised the national security of America's closest allies, including Australia's.

So I agree Hillary Clinton's assessment of the consequences of his Snowden's conduct, when she said recently:

"It puts people's lives in danger, threatens our national security, and undermines our efforts to work with other countries to solve shared problems."

Despite these threats and setbacks, it remains the case that liberal democracies like the US, UK and Australia lead the way in upholding values of individual liberty.

Significantly, the fundamental principles of governments upholding individual freedoms and ensuring national security do not have to be mutually exclusive. Instead, they should be seen as mutually complimentary – without security there can be no freedom. In his Jefferson Oration in Virginia on 4 July 1963 entitled 'The Battle for Freedom', Sir Robert Menzies, the Prime Minister of Australia stated:

"American history has reconciled both conceptions. For it has been your glorious destiny, notably in the turbulent years of the twentieth century, to evolve a system in which national power has grown on the basis of a passionate and Jeffersonian belief in individual freedom."

That attitude should always be the starting point in any debate about the perennial question of where, particularly at times of threat and danger, the balance is to be struck between the protection of public safety and the freedom of the individual. And it remains liberal democracies that continue to achieve that balance correctly today. No matter what the era, the most stable, open and transparent countries are liberal democracies, not those under authoritarian rule.

Many of the threats we face today are variations of known themes—military conflict, terrorism, crime or espionage. But globalisation and technological advancements mean the threats have evolved and that the challenge is now about international security, not just national security. Once more, we can expect them to continue evolving into the future. Most likely in ways we cannot entirely envisage today.

So, in the face of ever changing circumstances, how can we make a real difference in shaping our national security environment?

First, we must realise that no nation, no matter how large or powerful, can disrupt and prevent threats to global security alone. We must continue to work together and build large partnerships to counter the threat posed by those who would do us harm, whether offline or online. Our strength lies in our alliances and relationships with close and trusted partners. I believe there is no more important partner for Australia than the US and that the US has no readier or better friend than Australia.

However, the partnership cannot afford to only react to threats. In the current global environment, and post-Snowden period, there is a risk democratic states will play a waiting game. We cannot

afford to simply wait for the next world-changing event and then espouse how similar it really was to previous moments – this will only play into the hands of our adversaries, most likely be more expensive in the long term and risk the individual freedoms for which we have worked so hard.

The Australian Government is strongly committed to ensuring that Australian national security agencies have the resources they need to continue to achieve the significant outcomes we have experienced in protecting our most fundamental human rights—the right of our people to life, liberty and security of person.

We must continually work to address the gaps between technological progress and policy. This is true for all work of governments, but particularly so in the area of national security. Just as the technology employed by terrorists, agents of espionage and organised criminals adapts and advances, so too must the capabilities and powers of our law enforcement and security agencies. But this must always be done with the highest regard to ensuring proportionality to the threat and continued testing and maintenance of oversight mechanisms.

While our countries have different systems, we both share a commitment to individual freedoms. Progress in this area does not have to diminish our collective security, but can ensure appropriate oversight and smallest necessary encroachment on individual rights.

In a 2005 interview, former US National Security Adviser, Brent Scowcroft, said:

“America has never seen itself as a national state like all others, but rather as an experiment in human freedom and democracy.”

Australia is a much younger nation than the US, but our societies have evolved from common traditions. We share the same fundamental democratic values. Prime Minister Tony Abbott said of the United States during President Obama’s visit to Australia in 2011, *“no country on the earth has done more for the world”*.

For both of us, the liberty, as well as the security of our peoples, lie at the heart of national policy. We Australians will continue to work in close partnership with the American friends and allies to protect those values and to thwart those who would make it their cause to destroy our freedoms and to tear down our democracy.

For as Australians and Americans both know, we whose societies and systems had their inception in the values and optimism of the enlightenment will always prevail over the dark forces which would seek to do us harm.

© Copyright Attorney-General's Department 2013

Quelle: George Brandis: Securing Our Freedoms (speech delivered at the Center for Strategic and International Studies, Washington DC, 8.4.2014).

<http://www.attorneygeneral.gov.au/Speeches/Pages/2014/Second%20Quarter%202014/8April2014SecuringourFreedoms.aspx> (10.5.2015)

Dokument 4:

HOUSE OF REPRESENTATIVES

BILLS

Counter-Terrorism Legislation

Amendment Bill (No. 1) 2014

SPEECH

Monday, 1 December 2014

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

Monday, 1 December 2014 HOUSE OF REPRESENTATIVES 13711

CHAMBER

SPEECH

Date Monday, 1 December 2014 Source House

Page 13711 Proof No

Questioner Responder

Speaker Danby, Michael, MP Question No.

Mr DANBY (Melbourne Ports) (17:21): From the moment one enters this place, representing 100,000 constituents and their families, a sense of responsibility rests on one's shoulders. It is the gravity that in this place the decisions we make directly affect the security and safety of those who entrusted us to be here. Parliament has a responsibility to do all it can to maintain Australia's record of preventing a successful terrorist attack on mainland Australia and to prevent Australians from, and if necessary punishing Australians for, committing terrorist attacks overseas.

Last month, the Foreign Fighters Bill was referred to the Parliamentary Joint Committee on Intelligence and Security, who subsequently released 15 recommendations on the bill. I must commend many of the people, including the member for Hughes, who just spoke, and the members for Isaacs, Berowra and Holt, who pointed out that the joint committee had suggested the amendment of the bill to require: the AFP to provide the Attorney-General with a summary of the facts when seeking consent to apply to the court for an interim court order, including any facts indicating why such an order should not be made; the retention of the requirement for the AFP to explain to the issuing court the reasons for each condition in a draft control order, as the bill, as introduced, would have effectively reduced judicial oversight by not requiring the AFP to justify the control order as a whole; the shortening of the period for notification of the relevant minister where agencies issue emergency authorisations; and the government urgently to appoint a new Independent National Security Legislation Monitor. These are the sensible recommendations of people on the intelligence committee from all sides of parliament working maturely in the interests of their constituents. They are not those who seek to make political gain against the corporate wellbeing of their fellow Australian citizens.

My colleague Mark Dreyfus, the shadow Attorney-General and member for Isaacs, said earlier today in this

chamber:

... the recommendations will improve the accountability and transparency of decision making by national security agencies. The recommendations will also ensure that control order applications are closely and appropriately scrutinised.

Again, these are the mature actions of mainstream political parties—an issue I want to come back to when I refer to the contribution of the member for Melbourne.

It is a sad reality that a handful of Australians born, raised and educated—indeed, shaped—in Australia, as one of our speakers said, have taken it upon themselves to travel to Syria and Iraq to join a group that beheads captured enemies and slaughters men, women and children with any group that does not fit in with its perverse and perverted world view. It enslaves women and children for sexual gratification. It trades these victims with each other. Daesh kills people arrested for smoking or for playing music. They are systematically destroying millennia of Muslim antiquities across the Middle East, including recently blowing up the tomb of Jonah in Mosul—a tomb that has existed for more than 1,000 years. It is truly the march of the barbarians.

Tens of thousands of foreign fighters have gone to Syria to fight and to kill. Deluded, they imagine they are soldiers. They are not. They have none of the professionalism and code of conduct strictly and proudly maintained by the men and women in Australian uniforms. These people think they are fighting war for Islam. They are a disgrace to the names of the great soldiers of Islam, like Saladin and Kemal Ataturk, whose honour and honourable treatment of the enemies was praised even by their opponents. Daesh does not face much resistance when they come up against unarmed Christians, Yazidis and Shi'ites. They are slaughtered. Its shameful conduct and its victims are then boasted about on Facebook. Now, they are coming up against the US and Australian air forces and local fighters like the Kurdish Peshmerga, who are advised by our special forces. Nearly all MPs will wish the men and women of the ADF every success in suppressing these IS fighters, regardless of where they come from, including the cursed figures from this country who hold up the heads of locals they have killed and, even worse, who encourage their poor children to do the same.

The ADF has been the recipient of information from Australian intelligence services for years. This helps it do its job. The law, as currently rendered and which this legislation seeks to change, needlessly forces ASIS to jump through hoops to provide information to the ADF. The signals directorate and the DIO, which fall under the Defence minister's responsibility, do not have to jump through these hoops. But ASIS, which falls under the foreign minister's responsibility, does. All these organisations are on the same side. We in this parliament should be making it easier for them to do their job. As the member for Isaacs pointed out in his address today:

Australia's counter-terrorism efforts are supported by our open democratic society. There are inherent strengths in our society that make Australia resilient to the divisive worldview of al-Qa'ida—and Daesh. He also said:

More pages in the statute books will not make ours a more resilient community.

We know from experience that the terrorist narrative may resonate with a small number of Australians. It is incumbent upon all Australians to work together to reject the ideologies that promote violence no matter where

they arise or what purpose they aspire to. I praise in particular some courageous members of the Sydney Muslim community who have been at the forefront of this resilience project. Building this sort of resilience in the context of the foreign fighter threat is an even higher priority than when the white paper was written. This is a threat which is clearly increasing, as we have some 250 Australians, according to The Economist magazine, who wanted to participate either from this country or who are already over there. We have seen the damage that these kinds of people can do, as the member for Berowra pointed out, when one of the torturers from Daesh in Lebanon returned to Belgium and murdered four citizens in the capital of that country.

Remember why we are doing this. There were 88 Australians killed in the 2002 Bali bombing; 10 killed in the September 11 attacks; three killed in the 2009 Jakarta bombings; one killed and nine injured in the 2005 London bombings; two murdered by terrorists in the Mumbai terror attack; and one Australian, Malki Roth, killed in Jerusalem in 2001. Let us remember the report of the Council of Australia Governments, released in 2013, that said 35 Australians had been charged for terrorism offences, 26 of whom had been convicted. So we have a real problem overseas and a real problem with Australians who have already been affected by this.

Thank heavens, because of the work of this parliament, our security services and our military, we have not had a successful attack on mainland Australia. It is our responsibility as legislators on both sides of this great parliament to see that that continues, by passing legislation that will enable the ADF, ASIS and other people to work together to prevent that happening. This is not Hollywood. We are not basing our analysis, as the member for Melbourne seems to think, on the series Homeland. The proposed changes do not seek to change the ADF's rules of engagement.

The shadow Attorney-General and opposition have worked diligently to shape this and previous legislation that enhance the ability of our security services to work effectively and efficiently to stop these terrorists before they go there or to gather evidence about their activities while they are there. That way, when people return from the battlefield claiming they were in Syria for humanitarian reasons, they can be punished to the full extent of Australian law, and they ought to be. The necessity for acting on this problem arises from all of the reasons I have just set out. It includes the number of Australians who have already been killed in some of the terrible incidents, the number of people that are going over there to fight and the success of our laws—as the member for Berowra pointed out—in taking so many of those people who would seek to do these kinds of things in this country and under a system of law and arresting, charging and trying them and then having them convicted.

I want to end with this discordant note. It is not surprising to see the Greens political party lead the charge against this proposed legislation. In my view, the Greens seem to have an automatic Pavlovian kind of reaction to undermining the intelligence capabilities of our country. People like the Greens political party's Senator Ludlam have publicly supported self-appointed protectors of privacy and trust—stalwarts of moral standing like Julian Assange. Of course, the Greens' backing of Julian Assange and his ideological stablemate Edward Snowden has not exposed a single piece of evidence of the abuse of privacy or citizens' rights in authoritarian countries like Russia. Mr. Assange, the Greens' hero, used to host a program on the Russian disinformation network RT. To give you a flavour for his content and his policies, his first interview gave an armchair ride to Hezbollah's feared

terrorist leader, Sheikh Hussein Nasrallah.

Indeed, it is delicious irony that the Greens' other hero, Edward Snowden, preaches excessive oversight and accountability but chooses to reside in Russia, of all places. He destroyed his credibility when popping up on Russian TV a few months ago to give another soft-serve Dorothy Dixier to the new Russian tsar, Vladimir Putin. Perhaps the Greens believe Russia is actually a bastion of human rights. Certainly, Senator Rhiannon used to believe that. I am honoured with the fact that Senator Ludlum has put a fatwa on the Greens speaking to me because I pointed out Senator Rhiannon's political similarity to the wife of the Romanian dictator, Elena Ceausescu. But the main point I make about her is she has never dissociated herself from her membership and participation in the pro-Soviet Communist political party in Australia. It was a seamless transition to the Greens. Of course, the serious people in this parliament can smirk about Snowden's choice of patrons and about Assange's presence on RT. But it is hard to believe that here, in this House, we have parliamentarians that oppose legislation and seek to foil the efforts of our Defence forces and cooperation with our security services overseas. It occurs to me that the Greens political party ought to be more concerned about people losing their heads than about the people holding the swords. We had the appeasers in the 1930s. Eighty years later we have the Greens.

I have asked in this parliament a number of times why Mr Snowden and why the Greens support the release of material about how the Five Eyes, the Western intelligence services, intercepted telecommunications in northern Iraq prior to Daesh's conquering of that area. This is completely inimical to the safety of Western civilians. It has nothing to do with privacy. These questions have been raised by reputable publications like The Christian Science Monitor and The Washington Post. I fear that Daesh was able to change the pattern of its telecommunications as a result of the Snowden revelations in order to evade monitoring by security services like Australia's, like the American security services and like the British security services. Therefore, the pattern of murder and mayhem that they have wrought across northern Iraq has, in fact, been facilitated by the Snowden revelations, which were completely unnecessarily made about how we have intercepted telecommunications of terrorist organisations in northern Iraq.

This is a place to have serious debates about serious matters. Matters such as increasing the security services' capability do need scrutiny. They have had scrutiny at the intelligence committee by serious people who have come back to this parliament and made their recommendations. I congratulate the government and the opposition for our practical and judicious approach, including the shadow Attorney-General for his cooperation with the Attorney-General in the framing of these laws and the recommendations of the intelligence committee. These are matters too serious to be left to the mouthpieces of Assange, Snowden and the Greens who, once again, have proven their wish to continue their irresponsible approach to national security. When we use grandiose words like 'national security', what do we mean? We mean the safety of innocent Australian citizens—our constituents who we are duty bound to care for and to seek measures to protect from any incident happening here in Australia, as has happened to them overseas.

These are measured steps to see that the human rights, above all the right to security, of all Australians are enhanced in this additional piece of legislation. I commend it to the House. I commend the government and many

of the speakers who have been on this side, as well as the opposition, for considering the safety and security of Australians above all and, in a measured way, taking into consideration matters of civil liberties and privacy which were done by the intelligence committee in a very responsible way.

Quelle: Michael Danby: Speech, House of Representatives, 1.12.2014.

http://parlinfo.aph.gov.au/parlInfo/genpdf/chamber/hansardr/2d891fab-c2b5-41b4-967f-0b37fdb6fe7c/0168/hansard_frag.pdf;fileType=application%2Fpdf (21.5.2015)

Dokument 5:**Explained: Australia's involvement with the NSA, the US spy agency at heart of global scandal**

By [Tim Leslie](#) and [Mark Corcoran](#), ABC News

Updated 19 Nov 2013, 8:52am

The US National Security Agency (NSA) spying scandal was sparked by the release of documents by former NSA employee Edward Snowden.

The leaks caused outrage around the world, including in Australia where documents released by Snowden revealed Australia had been spying on its regional neighbours as part of a joint intelligence program with the US.

So why has the release had such a dramatic impact on global relations, and what are the implications for Australia?

What are the key global developments in the scandal?

Snowden, a computer analyst who worked as a contractor for the NSA, leaked details about the extent of top-secret surveillance programs undertaken by the US and its allies, including Australia and the United Kingdom.

Coming in the aftermath of the WikiLeaks scandal, an irate US government launched a global manhunt to track the source of the leaks.

Snowden, however, had been much more discreet with his communications, and was able to make it to Russia where he applied for asylum.

His leaks initially exposed the extent to which the US was gathering information on its own citizens, and prompted widespread calls for a rethink about the scope of intelligence monitoring.

The scandal took on an international element after allegations emerged that the NSA monitored the phone calls of 35 world leaders, including tapping the mobile phone of German chancellor Angela Merkel, and conducted widespread electronic snooping on a global scale.

The revelations resulted in a stinging rebuke from Ms Merkel, a close international ally of US president Barack Obama, who was forced to deny he was aware Ms Merkel's phone was tapped.

More recently the role of major technology companies in assisting the collection of data has come under scrutiny with allegations the NSA and its UK counterpart are copying large amounts of data from the fibre optic cables that internet giants such as Google and Yahoo use to communicate between their centres.

This information is likely fed into a NSA program called XKeyscore, which allows NSA staff to search through a vast amount of online information collected through various means.

Details about XKeyscore come from training materials leaked by Snowden, which outline the ease with which the NSA can gather information on a person's online activities if they have access to their email address.

What is Australia's involvement?

Further documents leaked by Snowden revealed details of Australian Government electronic spying throughout the Asia-Pacific region using a series of listening posts stationed in diplomatic missions.

A diplomatic dispute erupted in the region following a story released by Fairfax media, which reported a top-secret map detailing 90 US surveillance facilities at diplomatic missions worldwide - including in Cambodia, China, Indonesia, Malaysia, Myanmar and Thailand.

There have been further embarrassing revelations with the publication of top secret documents obtained by the ABC and Guardian Australia, from material leaked by Edward Snowden, showing details of an Australian intelligence operation to monitor the mobile phone of Indonesian president Susilo Bambang Yudhoyono over 15 days in August 2009.

The documents indicate that Australian intelligence sought a long term strategy to continuing monitoring the president's calls. Also on the leaked "Leadership Targets" list were the president's wife, the current and former vice presidents of Indonesia and other key figures in the President's inner circle.

The intelligence operation was conducted by the Australian Signals Directorate (ASD).

Leading intelligence academic and author Professor Des Ball of the ANU says Australia is party to the UKUSA intelligence agreement, also known as the Five Eyes - which divides the globe into collection areas. Australia has responsibility from the mid-Indian Ocean across to the western Pacific and northwards into southern China.

The UKUSA agreement was borne out of intelligence sharing between the US and the United Kingdom in World War II and extended to include Australia, Canada and New Zealand.

Its existence was allegedly so secret that prime ministers were unaware of the agreement until 1973 - the same year the Commonwealth raided ASIO in a shake-up of security agencies.

Professor Ball says the NSA receives intelligence from four key facilities in Australia that are part of the XKeyscore program.

One Snowden NSA document specifically mentioned operations taking place at "Australian diplomatic facilities", and alleges the ASD operated the listening posts from the embassies without the knowledge of most of the diplomats stationed there.

It also emerged that Australia and the US used the 2007 Bali Climate Change Summit to collect phone numbers of security officials in Indonesia.

The details are said to be in a January 2008 report from the NSA's Australia station at Pine Gap, a facility operated jointly with the CIA and the Australian Defence Department.

What is the Australian Signals Directorate?

While ASIO and ASIS most often spring to mind when thinking of Australian intelligence, the NSA monitoring scandal involves the Australian Signals Directorate (ASD) - an organisation within the Defence Department.

Employing more than 2,000 military and civilian staff, with an undisclosed budget believed to exceed several hundred million dollars a year, ASD is Australia's largest, most secretive intelligence agency.

But this shadowy world is less James Bond, more mathematician, with ASD employing technicians, analysts, code-breakers and linguists to operate what amounts to a vast digital vacuum cleaner, pulling in data from the ionosphere and cable networks.

From phone calls to near-obsolete faxes, ASD has the capability see, hear or read it all.

Its network includes large facilities near Geraldton, Darwin and Canberra, listening stations concealed within Australian embassies and consulates throughout the Asia-Pacific region, and remotely controlled outposts at Bamaga on the tip of Cape York and the Cocos Islands.

ASD also has a team at Pine Gap, the US facility, located in central Australia, and jointly operated by the NSA and the Central Intelligence Agency.

The onset of the digital age has only served to extend ASD's capability and accelerate the scale of collection, with banks of harvested metadata reportedly stored and processed at a new purpose built ASD facility at HMAS Harman near Canberra.

ASD is regarded by many senior Washington officials as Canberra's most valuable contribution to the US-Australian strategic alliance.

The ASD's motto is "Reveal their secrets, protect our own", so it is unsurprising it has been involved in the widespread data collection.

In recent years, ASD has partly emerged from the shadows to promote its other role in protecting Australian government communications. It also advises Australian businesses on protecting themselves from cyber-security threats.

However, its primary mission - targeting the diplomatic and military communications of neighbouring countries - remains highly classified.

The Snowden revelations that Australia has been spying on its neighbours from diplomatic missions have predictably been met with outrage from the countries named in the reports – despite journalists and academics progressively revealing details of these activities since the 1980s. Professor Ball says an earlier diplomatic spying operation was conducted under the codename *Relieve*, which intercepted local phone calls relayed by microwave link.

In 1988, details first emerged of another more sophisticated global eavesdropping system *Echelon*, which gave the UKUSA partners, including Australia, global access to satellite and phone communications.

In 1995 the ABC and the Sydney Morning Herald revealed a highly sophisticated joint US-Australian operation to bug the newly constructed Chinese Embassy in Canberra. So sensitive was this mission that prior to publication - and despite widespread knowledge of the bugging in diplomatic circles - the Australian government unsuccessfully attempted to suppress media publication of the operation.

What has the regional reaction been to the Snowden revelations?

Prime Minister Tony Abbott would not be drawn on the latest revelations of ASD spying on the Indonesian president, telling the Australian Parliament that all governments gather intelligence and Australia only uses the information to help allies.

But Mr Yudhoyono's reaction was swift: he recalled Indonesia's ambassador to Australia, and issued a series of scathing tweets accusing the US and Australia of "wounding the strategic partnership with Indonesia."

Former Australian diplomat Bruce Haigh says the public revelations of Australian spying mean Indonesia has lost face.

But he says Australia's relationship with Indonesia is quite strong and "will survive" the revelations.

Former defence intelligence analyst turned independent Federal MP Andrew Wilkie said "we've got to be realistic here".

"The foreign intelligence services of Australia and, in fact, near on every other country in the world conduct intelligence collection operations against foreign targets. In a perfect world, that wouldn't happen, it wouldn't be necessary, it wouldn't go on. But it is not a perfect world and it does have to happen and it does happen."

Responding to the earlier revelations that Australia had used its embassies for signals intelligence gathering, Malaysia summoned the Australian ambassador to express its discontent over the allegations, while China publicly warned foreign embassy staff it was illegal to engage in monitoring activities.

Since the Bali bombings Australia and Indonesia have increasingly shared intelligence in the fight against regional terrorism, but after failing to secure answers from the Australian or US

governments, Dr Natalegawa has signaled this intelligence sharing will be reviewed in light of the scandal.

Australian Foreign Minister Julie Bishop has so far refused to comment on the allegations, saying she will not publically discuss intelligence matters, but the allegations overshadowed her trip to Indonesia for the Bali Democracy Forum.

What is the problem with intercepting communications - isn't this what spies do?

Despite the vocal protests from governments around the world, the contents of the Snowden leaks are unlikely to have come as a surprise to leaders and government decision makers.

Much of the reaction stems from the embarrassment of the spying being made public – with leaders such as Ms Merkel likely reacting more to placate domestic audiences.

Former Mexican president Vicente Fox, free from the constraints of office, offered perhaps a more honest answer to the impact of the allegations saying "of course" he was spied on when he was in power.

"It's nothing new that there's espionage in every government in the world, including Mexico. I don't understand the scandal," he told a Spanish radio station.

However, the scale of the data collected, both on US citizens and globally, raises serious questions about the need to address the new realities of the information age.

The amount of recorded information on individuals is greater and has more potential to do harm than ever before, and technology has removed the barriers of scale that previously hampered mass surveillance.

For the first time tools exist to make sense of the vast swathes of information collected and to tie that information to an individual.

The implications for Australians also likely go beyond the NSA's program. Professor Ball says he expects the ASD is gathering similar information on Australian citizens.

Why did Indonesia make such a big deal about the embassy story?

Sam Roggeveen, the editor of the Lowy Institute's Interpreter magazine, and a former Australian government intelligence analyst, offers his thoughts on why Indonesia has reacted this way:

Last week I admitted to being a bit baffled by the Indonesian government's decision to make such a big deal about a minor Australian news story on electronic eavesdropping from Australian diplomatic facilities

If anything, the Indonesians have escalated the dispute since then, with foreign minister Natalegawa saying the row may threaten cooperation on people smuggling, and some Indonesian MPs taking the opportunity to create mischief.

Given that the sort of intelligence activity described in the original Fairfax story is common knowledge, why is Indonesia making a fuss?

A run-down of the various theories, some of which have appeared in the media and others which I have heard privately:

1. Softening Australia up. This one is courtesy of former Lowy Institute executive director Michael Wesley in The Guardian:

Natelagawa, who studied in Australia, has probably watched the odd State of Origin game. He knows the first 10 minutes of the match are known as the "softening up period" - a stanza of ferocious physicality in which each side tries to cow the opposition into a disadvantageous state of mind. Right now, there's a new government in Canberra, and neighbouring governments are likely to be keen to test its mettle. The odd diplomatic jab can give a better sense of what can be expected from a new government than years of polite cocktail discussions.

2. SBY has a grudge. This theory holds that, although Dr Natalegawa is taking the lead on this issue, it is at the direct instruction of president Susilo Bambang Yudhoyono, although his motives are unclear.

3. Mr Natalegawa is making up with his boss. This theory holds that SBY was displeased that Dr Natalegawa allowed a transcript of his New York meeting with Ms Bishop to be leaked (it was the leaking that upset him, not the damage to the Australia relationship). Dr Natalegawa has seized on the spying issue so that he can appear statesmanlike and get back in SBY's good books.

4. The domestic audience. As reader Neil Watson said last week: "We can expect more of this in the run up to next year's presidential election. I'd suggest SBY is also pre-empting the xenophobes in the parliament and 'think tanks' who will be demanding firm measure. It is also a diversion from the corruption allegations surrounding the Democrat Party."

5. The colonial legacy. Ian Brownlie, in his reader riposte earlier this week, argued that "the particular factor in Indonesia's case is the knee-jerk sense of victimhood from exploitation by wealthier, stronger outsiders seen subconsciously or consciously as neo-colonialist invaders. The Germans may admit that spying is something they also do; for Indonesians, it can only be something that others do to them".

6. Indonesia is angry with Australia. Last, let's not ignore the possibility that Indonesia is genuinely annoyed with Australia. It is one thing to know that spying goes on, but another to be confronted with specific facts about foreigners snooping on you in your own capital.

Mr Roggeveen's analysis first appeared on the Lowy Institute's Interpreter website. Quelle: Tim Leslie/Mark Corcoran: Explained: Australia's involvement with the NSA, the US spy agency at heart of global scandal, ABC News, 19.11.2013. <http://www.abc.net.au/news/2013-11-08/australian-nsa-involvement-explained/5079786> (10.5.2015)

Dokument 6:Surveillance**Revealed: Australian spy agency offered to share data about ordinary citizens**

- Secret 5-Eyes document shows surveillance partners discussing what information they can pool about their citizens
- DSD indicated it could provide material without some privacy restraints imposed by other countries such as Canada
- Medical, legal or religious information 'not automatically limited'
- Concern that intelligence agency could be 'operating outside its legal mandate'

Ewen MacAskill, James Ball and Katharine Murphy, The Guardian Australia

Monday 2 December 2013 11.20 AEDT Last modified on Tuesday 3 December 2013 11.30 AEDT

Australia's surveillance agency offered to share information collected about ordinary Australian citizens with its major intelligence partners, according to a secret 2008 document leaked by the US whistleblower Edward Snowden.

The document shows the partners discussing whether or not to share "medical, legal or religious information", and increases concern that the agency could be operating outside its legal mandate, according to the human rights lawyer Geoffrey Robertson QC.

The Australian intelligence agency, then known as the Defence Signals Directorate (DSD), indicated it could share bulk material without some of the privacy restraints imposed by other countries, such as Canada.

"DSD can share bulk, unselected, unminimised metadata as long as there is no intent to target an Australian national," notes from an intelligence conference say. "Unintentional collection is not viewed as a significant issue."

The agency acknowledged that more substantial interrogation of the material would, however, require a warrant.

4. **CSEC** are able to make use of unselected (comment do we need to define "selected" and "unselected" and "unintentional" in the context of this section. As I

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

SECRET//20320108

SECRET//20320108

<File Reference number>

recall, it was important that we all understand what we mean by such terms) metadata for developing their capability. However, bulk, unselected metadata presents too high a risk to share with second parties at this time, because of the requirement to ensure that the identities of Canadians or persons in Canada are minimised, but re-evaluation of this stance is ongoing .

5. **DSD** can share bulk, unselected, un-minimised metadata as long as there is no intent to target an Australian national – unintentional collection is not viewed as a significant issue. However, if a 'pattern of life' search detects an Australian then there would be a need to contact DSD and ask them to obtain a ministerial warrant to continue.

Metadata is the information we all generate whenever we use technology, from the date and time of a phone call to the location from which an email is sent.

"Bulk, unselected, unminimised metadata" means that this data is in its raw state, and nothing has been deleted or redacted in order to protect the privacy of ordinary citizens who might have been caught in the dragnet. Metadata can present a very complete picture of someone's life.

The working document, marked secret, sheds new light on the extent to which intelligence agencies at that time were considering sharing information with foreign surveillance partners, and it provides further confirmation that, to some extent at least, there is warrantless surveillance of Australians' personal metadata.

The DSD joined its four intelligence-sharing partners – the US, Britain, Canada and New Zealand, collectively known as 5-Eyes – to discuss what could and what could not be shared under

the different jurisdictions at a meeting hosted by Britain's GCHQ at its headquarters in Cheltenham on 22-23 April, 2008.

The notes, published today by Guardian Australia, suggest that Australia was open to pooling bulk data that almost certainly includes information about Australian citizens.

Clearly indicating the different attitudes between the intelligence partners, the Canadians insisted that bulk collection could only be shared if information about its citizens was first "minimised", meaning deleted or removed. The various techniques used in "minimisation" help protect citizens' privacy.

The GCHQ memo taker, reporting on this, said that "bulk, unselected metadata presents too high a risk to share with second parties at this time because of the requirement to ensure that the identities of Canadians or persons in Canada are minimised, but re-evaluation of this stance is ongoing".

By contrast, DSD, now renamed the Australian Signals Directorate, offered a broader sweep of material to its partners.

DSD offered to share bulk, unselected, unminimised metadata – although there were specific caveats. The note taker at the meeting writes: "However, if a 'pattern of life' search detects an Australian then there would be a need to contact DSD and ask them to obtain a ministerial warrant to continue."

A "pattern of life" search is more detailed one – joining the dots to build up a portrait of an individual's daily activities.

It is technically possible to strip out the metadata of Australian nationals from bulk collection methods used by the 5-Eyes countries, such as cable taps – ensuring the information is not stored, and so could not be pulled in to searches and investigations by agents.

The Snowden documents reveal Australia's intelligence services instead offered to leave the data in its raw state.

Australian politicians have insisted that all surveillance undertaken is in accordance with the law.

But Geoffrey Robertson, writing in the Guardian today, says if what was described in the memo took place, this would be a breach of sections eight and 12 of the Intelligence Services Act 2001. The act sets a strict requirement that ministerial authorisation is required if the data of an Australian citizen is involved, and indicates that the citizen must be a "person of interest", such as someone involved in terrorism or organised crime.

The Cheltenham gathering, which appears to have been convened to consider the issues around the burgeoning collection of metadata and to reach common positions, resolved to avoid pre-emptive efforts to categorise various materials and "simply focus on what is shareable in bulk".

The memo flags privacy concerns around the collection of various types of data, but the meeting, according to the record, resolved not to set "automatic limitations" – leaving judgment calls to each country's own agencies.

"Consideration was given as to whether any types of data were prohibited, for example medical, legal, religious or restricted business information, which may be regarded as an intrusion of privacy," the memo says.

"Given the nascent state of many of these data types then no, or limited, precedents have been set with respect to proportionality or propriety, or whether different legal considerations applies to the 'ownership' of this data compared with the communications data that we were more accustomed to handle."

"It was agreed that the conference should not seek to set any automatic limitations, but any such difficult cases would have to be considered by 'owning' agency on a case-by-case basis."

12. Consideration was given as to whether any types of data were prohibited, for example medical, legal, religious or restricted business information, which may be regarded as an intrusion of privacy. Given the nascent state of many of these data types then no, or limited, precedents have been set with respect to proportionality or propriety, or whether different legal considerations applies to the "ownership" of this data compared with the communications data that we were more accustomed to handle. It was agreed that the conference should not seek to set any automatic limitations, but any such difficult cases would have to be considered by "owning" agency on a case-by-case basis.

The document also shows the agencies considering disclosure to "non-intelligence agencies". It says: "Asio and the Australian federal police are currently reviewing how Sigint [signals intelligence] information can be used by non-intelligence agencies."

48. DSD do not share SIGINT metadata outside COMINT channels as there is no expectation on them to do so. There is pressure to provide survey work to the military, and in future DSD may be required to release SRI at non-codeword levels. ASIO and Australian Federal Police are currently reviewing how SIGINT information can be used by non-intelligence agencies.

The record of the Cheltenham meeting does not indicate whether the activities under discussion in April 2008 progressed to final decisions or specific actions. It appears to be a working draft.

Since Snowden leaked the NSA documents to the Guardian and the Washington Post in May, controversy has raged around the world over revelations that surveillance agencies are collecting information in bulk about ordinary citizens' day-to-day activities, without first getting a warrant.

In Australia, the Greens party and the South Australian independent senator Nick Xenophon have been pursuing questions about the extent to which Australian citizens have been caught up in the dragnet, and the extent of Australian intelligence agencies' involvement.

So far, those questions have largely met with stonewalling, both under the previous Labor government and the new Abbott administration.

Quelle: Ewen MacAskill/James Ball/Katahrine Murphy: Revealed: Australian spy agency offered to share data about ordinary citizens, The Guardian, 2.12.2013.

<http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens> (21.5.2015)

Dokument 7:

George Brandis in 'car crash' interview over controversial data retention regime

Sydney Morning Herald, August 7, 2014 Ben Grubb Technology editor

Attorney-General George Brandis struggles to explain the government's proposed metadata retention laws in a Sky News TV interview.

It's been called "excruciating" and "the most embarrassing interview you'll ever be likely to see".

Attorney-General George Brandis struggled to explain live on Sky News on Wednesday afternoon the details of his government's controversial "data retention" policy, which would force all telcos to keep logs on what their customers do on the phone and online for up to two years, so law enforcement agencies could access the information without a warrant when investigating crime.

Earlier in the day, Prime Minister Tony Abbott said the policy would capture "the sites you're visiting". But his office later clarified this was not the case and that this would require a warrant.

Now Senator Brandis has confused matters again, telling Sky News that web addresses would be captured by his proposal to strengthen the powers of law-enforcement and intelligence agencies.

After repeated questions over whether the sites people visited would be captured, he conceded they would be, but confusingly contradicted himself by saying his policy wouldn't extend to web surfing.

He then attempted to clarify this by saying that the sites people visited would be captured, but not the individual web pages a person navigated to within a site.

Asked if metadata from sites such as Twitter and Facebook would also be captured, Senator Brandis said the extent to which social media would be involved was something that was still "under discussion".

Twitter users immediately mocked the interview.

"What an absolutely glorious train wreck of an interview," wrote one.

"Brandis has no idea what he's talking about on data retention," said another.

"Complete car crash interview with Brandis and @David_Speers [on] @SkyNewsAust as he tries to explain metadata," said yet another.

Steve Dalby, the chief regulatory officer at iiNet, an internet provider that is against the government's data retention proposal, called the interview "as clear as mud".

He's called on the government to release exactly what data they are after under the data retention proposal before it is legislated later this year.

The government did not have the best day in selling the proposal on Wednesday, with contradictory statements and broken metaphors used to explain the issue.

When describing that "web addresses" would be captured, it's possible Senator Brandis meant to say that the IP addresses of web servers people accessed would be stored.

When a web user visits Google, for instance, the IP address left behind as metadata is 74.125.237.198. When visiting Sky News, it's 101.167.166.43.

But if a law enforcement agency accessed this IP address metadata and put it into a web browser they would then be able to determine that the user went to Google or Sky.

Law enforcement or intelligence officials would also be able to determine the duration of time a user spent on the sites, the date they visited them, and the location of the device they visited the sites on.

The same applies to some other sites, but not all. In many smaller website hosting environments for instance, a single IP address might service hundreds of completely different and independent websites. This means that an IP cannot be considered a full web browsing history.

Mr Dalby told Fairfax Media on Wednesday evening that storing IP addresses was very similar to storing web browsing histories.

"[Law enforcement agencies] only have to type the damn IP address [into a web browser] and they'll get the website [you were looking at and] they'll get all the content on it," Mr Dalby said.

"It's just as invasive as standing with a video camera over my shoulder while I'm browsing and of course that's what they want," Mr Dalby said.

Mr Abbott's recently appointed Human Rights Commissioner, Tim Wilson, is also against data retention, as are a number of other civil liberties groups.

"I don't support the idea of data retention at all but I do realise that there are ways that it can be more or less infringing on peoples' right to privacy," Mr Wilson told Fairfax.

Senator Brandis' interview is reminiscent of an interview Mr Abbott gave in opposition when attempting to describe the broadband policy he was trying to take to the 2010 election.

He said then he was "no Bill Gates" and "no tech head".

August 07, 2014, 8:03AM Copyright © 2015 Fairfax Media Quelle: Ben Grubb: George Brandis in 'car crash' interview over controversial data retention regime, Sydney Morning Herald, 7.8.2014. <http://www.smh.com.au/digital-life/digital-life-news/george-brandis-in-car-crash-interview-over-controversial-data-retention-regime-20140806-101849.html> (10.5.2015)

Dokument 8:

Journalists will face jail over spy leaks under new security laws

George Brandis's new spying laws will include measure to criminalise media reporting of Snowden-style leaks

Paul Farrell and Daniel Hurst

Wednesday 16 July 2014 21.55 AEST Last modified on Thursday 17 July 2014 09.45 AEST

Australian journalists could face prosecution and jail for reporting Snowden-style revelations about certain spy operations, in an "outrageous" expansion of the government's national security powers, leading criminal lawyers have warned.

A bill presented to parliament on Wednesday by the attorney general, George Brandis, would expand the powers of the Australian Security Intelligence Organisation (Asio), including creation of a new offence punishable by five years in jail for "any person" who disclosed information relating to "special intelligence operations".

The person would be liable for a 10-year term if the disclosure would "endanger the health or safety of any person or prejudice the effective conduct of a special intelligence operation".

Special intelligence operations are a new type of operation in which intelligence officers receive immunity from liability or prosecution where they may need to engage in conduct that would be otherwise unlawful.

The bill also creates new offences that only apply to current and former intelligence operatives and contractors in a move which appeared to directly address the risk of documentary disclosures being made following revelations by the US National Security Agency whistleblower Edward Snowden – whom Brandis has previously labelled a "traitor".

On Thursday Brandis dismissed suggestions he was specifically going after journalists who reported information.

"No we're not and I think there has been a little bit of erroneous commentary on that provision," Brandis told the ABC.

"It's designed to plug a gap in the existing legislation. Under the existing legislation it's a criminal offence for an officer of a national security agency to disclose intelligence material to a third party, but it's not an offence for an officer to copy or wrongfully remove that material.

"In other words, communication with a third party is an element of the current offence but it seems to us that it should be wrong and it should be an offence to illicitly remove intelligence material from an agency. That's all that's about."

But the leading criminal barrister and Australian Lawyers Alliance spokesman Greg Barns said a separate provision in the “troubling” legislation could be used to prosecute and jail journalists who reported on information they received about special intelligence operations.

The offences relating to the unauthorised disclosure of information are outlined in section 35P of the national security legislation amendment bill, which was presented to the Senate on Wednesday and is set to face parliamentary debate after the winter recess.

The explanatory memorandum to the bill said the offence applied to “disclosures by any person, including participants in an SIO [special intelligence operation], other persons to whom information about an SIO has been communicated in an official capacity, and persons who are the recipients of an unauthorised disclosure of information, should they engage in any subsequent disclosure”.

Barns said: “I thought the Snowden clause [in the bill] was bad enough but this takes the Snowden clause and makes it a Snowden/Assange/Guardian/New York Times clause.”

“It’s an unprecedented clause which would capture the likes of Wikileaks, the Guardian, the New York Times, and any other media organisation that reports on such material.”

Barns, who has worked on terrorism cases and has also advised Wikileaks, said Asio could secretly declare many future cases to be special intelligence operations. This would trigger the option to prosecute journalists who subsequently discover and report on aspects of those operations.

He said it would be easy for Asio to declare special intelligence operations because it simply required the security director-general or deputy director-general to approve.

“Their own boss says, ‘I think we better call this a special intelligence operation, don’t you?’ ‘Yes, sir,’ close it down. The more you talk about it the more outrageous it becomes,” Barns said.

Barns said operations in which Asio officers broke laws were the very ones that the community may regard as abuses of power. He argued Brandis wanted powers not available to governments in the UK and the US where citizens enjoyed greater protections for freedom of speech.

“In Australia we lack that fundamental human rights protection and therefore Brandis can get away with inserting a clause into a bill which you wouldn’t be able to do in the UK or in the US,” Barns said.

“It’s the sort of clause you’d expect to see in Russia or in China and in other authoritarian states but you don’t expect to see it in a democracy. I hope the Senate rejects it because it takes the law further than in jurisdictions which are similar to Australia.”

Leading criminal law barrister Shane Prince said the new offences relating to special operations were “quite draconian”.

“The five-year offence would seem to be able to apply even if the person had no idea about the special intelligence operation and they happened to release information which coincidentally was part of or related to the special intelligence operation,” he said.

“Add on to that the fact you probably in a trial wouldn’t be able to know what the special intelligence operation was about, would mean that you could have the situation where a person could be on trial for disclosing information which they say is related to a special intelligence operation, even if the person didn’t know that the information related to a special intelligence operation and they would never get to know in their trial.”

The Greens senator Scott Ludlam said the new offence could criminalise the actions of journalists. “I can’t see anything that conditions it or carves out any public interest disclosures. I can’t see anything that would protect journalists,” he said.

Electronic Frontiers Australia chief executive Jon Lawrence said the clause covering security personnel “appears to be a clear attempt to stamp down on whistleblowers to avoid an Australian Ed Snowden.

“The fact that they’re making that illegal doesn’t necessarily stop a whistleblower though I think in the general context of what is a pretty extreme crackdown on whistleblowers generally.”

The amendments would explicitly bring private contractors under the definition of intelligence operatives to make them subject to prosecution, and include any person “performing functions or services for the organisations in accordance with a contract, agreement or other arrangement”.

The new penalties criminalise copying, transcribing, retaining or recording intelligence material in any way, and carry a maximum penalty of three years. Evidence of disclosure is not required for these penalties.

Brandis said this measure filled a gap in existing legislation whereby it was not unlawful for an officer of Asio to illicitly copy or remove material from Asio. He said it was already an offence for officers to disclose confidential information to a third party, punishable by up to two years in jail, and that penalty would increase to 10 years.

The president of the NSW Council for Civil Liberties, Stephen Blanks, said the penalties raised serious concerns.

“When things go awry total secrecy is not desirable. When something is seriously awry whistleblowers play a vital role in the provision of good governance. The recent case relating to East Timor has thrown some light on this balance in Australia.”

The bill is the first element of the government’s planned national security reforms, with further changes set to target the risk posed by Australians who fight in Syria and Iraq and then return home.

Independent MP Andrew Wilkie, a former intelligence analyst, said on Wednesday it was important for intelligence officers to be able to make public interest disclosures. Australia's whistleblower legislation leaves a narrow window for disclosure of intelligence information.

"It must be accompanied by protection for intelligence officials who copy and disseminate material in the public interest," Wilkie said.

Brandis referred the bill to the parliamentary joint committee on intelligence and security for a report by September, when MPs are set to debate the law.

Quelle: Paul Farrell/Daniel Hurst: Journalists will face jail over spy leaks under new security laws, The Guardian, 16.7.2014. <http://www.theguardian.com/world/2014/jul/16/journalists-face-jail-leaks-security-laws> (10.5.2015)

Dokument 9:



Sign the petition

Right now the government is considering radical changes to Australia's surveillance and intelligence laws. Of course authorities should be given the powers they need to protect us, but what's being considered goes much further than is necessary.

Police and intelligence agencies already have broad powers to request that information about the communications of specified individuals be retained to support their investigations.

What they're seeking now is for that information to be retained for two years for **ALL Australians**, even if you're not being investigated.

Though the government's initial attempts to articulate what their data retention regime will include have been disastrous, we do know that they want the following information retained:

- **Phone calls:** detailed records of phone calls you make and receive, including the two numbers. If a mobile phone is involved, that will include the location of that phone, resulting in a detailed record of your location and movements being collected. [See this example](#) to understand just how revealing this information can be.
- **Email:** detailed records of who you're sending emails to and receiving them from.

Are details of web browsing to be included?

Watch the Attorney-General's attempt to answer that question. Since this interview, the government has clarified that they do not wish to collect and retain details of web browsing.

But they do want to retain a record of the address assigned to your connection when you access the Internet (called an originating IP address). This information will allow the police and ASIO to identify who has visited specific websites that are of interest to them. It will also allow copyright owners (via subpoena) to identify people they believe are infringing their copyright, by downloading or file-sharing.

Even without web browsing information included, a mandatory, society-wide data retention regime represents a massive invasion of the privacy of all Australians. It also subverts the principle of presumption

of innocence by treating us all as potential suspects.

There will be substantial costs associated with implementing such a regime, and guess who'll be paying? Yep, you will: one estimate is that it will add \$100 per year to each internet bill.

The massive databases of highly sensitive (and valuable to organised criminals) information will also be highly prone to hacking and misuse, posing genuine threats to the safety of many Australians.

There are already more than sufficient powers available to Australia's intelligence and law enforcement agencies to have information retained about communications involving 'persons of interest'. There is no justification for this information to be retained on the rest of society.

Call on the Federal Government to drop its proposed mandatory, indiscriminate data retention regime, and to treat ordinary, law-abiding Australians as Citizens, Not Suspects.


*Known as 'data preservation notices'.

SOUND THE ALARM!

Tell your friends about the attack on our right to privacy.

Copy the link to IM, Skype or post it!

[Return to the Citizens, Not Suspects campaign page](#)

Text and the Citizens, Not Suspects image on this page are © Electronic Frontiers Australia Inc. and are licensed under a  [Creative Commons Attribution 4.0 International Licence \(CC BY 4.0\)](#)

[View EFA's Privacy Policy](#)

SIGN THE PETITION

We call on the Federal Government to drop its proposed mandatory, indiscriminate data retention regime, and to treat ordinary, law-abiding Australians as citizens, not suspects.

5,897 signatures We need 4,103 more

Quelle: Citizens Not Suspects: Online-Petition.
<https://www.getup.org.au/campaigns/privacy/mandatory-data-retention-efa--2/sign-the-petition> (10.5.2015)