Submission No 146

Inquiry into potential reforms of National Security Legislation

Name: Senator Scott Ludlum

SENATOR SCOTT LUDLAM
AUSTRALIAN GREENS
SENATOR FOR WESTERN AUSTRALIA

Submission to the Joint Committee on Intelligence and Security on potential reforms of National Security Legislation

Introduction

The Australian Greens welcome this Inquiry for providing an opportunity for public input and scrutiny of proposed reforms to national security legislation. Some of the proposals are dangerous, unnecessary and not proportionate to threats faced. However, examining proposals, principles and options through an Inquiry is far preferable to recent practice in which increasingly expansive and poorly defined surveillance powers are rushed through the Parliament with minimal debate.

The Greens encourage the Committee to resist pressure to hastily report to the Attorney General, but rather examine the submissions and evidence provided by experts and citizens thoroughly. It was inappropriate for the Committee to set a 25-working day deadline for submissions, given the complexity of the legal and technical issues involved and broad scope of the Terms of Reference and Discussion Paper. While the additional two-week period granted by the Committee is helpful, the public should have been granted at least the two months it took the Committee to finally agree to the six-page Terms of Reference for this Inquiry.

The Australian Greens do not accept the Government's premise that the current interception regime resembles the structure of the industry and technology reminiscent of 1979 when the original *Telecommunications Interception and Access Act* (TIA) was created. It would appear that on the one hand, the government insists that more amendments are required to help our law enforcement agencies do their vital work and keep the regime up to date, yet on the other hand warns that the complexities arising from the amendments might lead to the Act being used in ways the Parliament didn't intend.

The *TIA Act* has been amended no less than 45 times since September 2001, including allowing interception of electronic communications in order to protect computer networks, or in order to combat cybercrime or acts of terrorism. However, the *TIA Act* annual report showed law enforcement and other agencies obtained nearly a quarter of a million authorisations for access to telecommunications information in 2010-11. Only a tiny fraction of these intercepts related to organised crime or counterterrorism work. The *ASIO Act 1979* has been amended 25 times since 11 September 2001**.** A schedule documenting these amendments is provided in Annex 1.

The Greens encourage the Committee to examine each proposal through a human rights lens. Human rights safeguards cannot be delivered merely through adding an objects clause to a Bill. While adding an objects clause can sharpen scope and interpretation, appropriate human rights and privacy safeguards must be enforceable through strict and detailed procedures, routinely operationalised and then validated by adequately resourced oversight and accountability mechanisms. It is precisely because interception is an erosion of human rights and privacy that it has been conditional on judicial approval, specific targets and for serious offences.

The Committee was requested to have regard to whether the proposed responses contain "appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector."

The Committee should be guided by the resolution adopted by the UN Human Rights Council on 5 July 2012 and reaffirmed by the UN General Assembly on 29 June 2012, and the 10 August 2011 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. This resolution focused on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the internet. These documents are provided in Annex 2 and 3.

The Rapporteur underscores the importance of the role of governments in fully guaranteeing the right to privacy of all individuals, without which the right to freedom of opinion and expression cannot be fully enjoyed. The Rapporteur emphasised that, "States are obliged to guarantee a free flow of ideas and information and the right to seek and receive as well as to impart information and ideas over the Internet. States are also required under international law to prohibit under its criminal law the following types of content: (a) child pornography; (b) direct and public incitement to commit genocide; (c) advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; and (d) incitement to terrorism. However, the Special Rapporteur reminds all States that any such laws must also comply with the three criteria of restrictions to the right to freedom of expression, namely: prescription by unambiguous law; pursuance of a legitimate purpose; and respect for the principles of necessity and proportionality."

Online safety, as well as privacy and civil liberties can be enhanced through getting the combination of legal, technical and cultural initiatives right. As much as it is the Government's role to promote collective protection against identity theft, online crime and acts of political violence, Australian citizens have a legitimate expectation that the government will defend their democratic right to privacy, freedom of expression, and freedom from arbitrary acts of state coercion. This is especially the case when the blurring of terrorism with civil disobedience and healthy dissent has seen our security agencies and police forces deployed against climate change demonstrators, the Occupy movement, anti-whaling campaigners, and supporters of the WikiLeaks publishing organisation.

Surveillance regimes and procedures are already being targeted at people and groups unrelated to national security threats and have eroded Australia's enjoyment of Article 19 of the Universal Declaration of Human Rights. This reads, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers".

The Discussion Paper provided by the Attorney General, *Equipping Australia Against Emerging and Evolving Threats*, does not provide adequate justification for further erosion of Article 19 rights. While the Attorney General has asked the Committee's views on retaining all data on all internet users for a period of two years, the paper does not make the case as to why this is necessary. Nor has it sufficiently examined the security risks posed by the misuse of the preserved data.

Proposals the Government *Wishes to Progress*

Strengthening safeguards and privacy protections of the *Telecommunications Interception and Access* Act

The Greens support the strengthening of safeguards and privacy protections under the *TIA Act*.

The *TIA Act* annual report showed law enforcement agencies requested nearly a quarter of a million authorisations for access to telecommunications information of Australians in 2010-11.The Greens are concerned by this colossal number. Given that Australia's security agencies and police forces have been deployed against targets that fall well beyond threats to national security such as climate change demonstrators, the Occupy movement, anti-whaling campaigners, and supporters of the WikiLeaks publishing organization, the lines between terrorism, civil disobedience, and healthy dissent are being routinely blurred. The number of intercepts could signal that current safeguards and privacy protections are insufficient.

The Australian Law Reform Commission (ALRC) has recommended that the Telecommunications Interception Act be reviewed in its entirety. The Greens strongly support the ALRC as the independent statutory authority with expertise in legal and human rights standards that could clarify, improve and build confidence in the regime and the appropriate oversight arrangements by the Commonwealth and State Ombudsmen.

Recommendation 1: The Committee is encouraged to make a reference to the ALRC for a thorough inquiry as per Recommendation 71-2 of ALRC Report 108 of August 2008.

Reforms to lawful access

The Attorney General's Terms of Reference and Discussion Paper uses vague terminology throughout and repeatedly urges streamlining and standardisation in the name of reducing complexity and enhancing efficiency. These terms carry positive connotations; however, making interception easier is not inherently good. It is appropriate for each intrusion into a citizen's communications to be scrutinised by a judicial authority, for the suspected crime to be serious and for the agency to be suitably skilled and equipped to handle this responsibility.

The Greens are opposed to any "modernisation" that leads to a lowering of the standards of tests or thresholds for intrusions into the privacy of Australians.

While reducing the number of agencies eligible to access communications sounds appropriate on the one hand, another proposal indicates that information sharing among agencies will be simplified, possibly leading to the same number (16 agencies currently) or potentially more entities having access to materials yielded through interception.

The Attorney General's paper does not explain what the problems are with the current system but alerts to the fact that currently agencies that do not have a demonstrated need to access information are currently eligible to do so.

Recommendation 2: The Committee is encouraged to seek clarification as to which agencies do not have a demonstrated need for information, the agencies proposed to have access to communications, and the agencies that might gain access through sharing arrangements.

The Attorney's paper alerts readers to the fact that child exploitation offences are currently not considered serious enough in Australian law, contrary to community standards. Rather than reducing the threshold for surveillance for all Australians, provisions pertaining to crimes against children should be modernised to appropriately punish offenders, and implement increased penalties.

Recommendation 3: The Committee should encourage the Attorney General to increase penalties for child exploitation offences.

The TIA Act's cost sharing arrangements & ACMA's role

While there is merit in principle to a tiered model, more precise information is needed on what costs sharing arrangements would apply when the Government alters the interception regime. The Greens are cautious of measures that would inhibit the emergence of new smaller ISPs and believe that the cost burden should be principally carried by government.

The status of ACMA is in flux. Depending upon the government's response to recommendations in the Convergence Review, it may not exist for much longer in its current form and may have significantly enhanced responsibilities for media regulation in the public interest. Additional responsibilities for the agency currently known as ACMA may not be appropriate depending upon its new configuration.

The Greens certainly agree that clarity is needed about ACMA's role under the TIA. It is not entirely clear how the number of disclosures of existing information or documents (549,859) stated in the ACMA 2010-11 Annual General Report relate to the number of authorisations (243,631) made for access to existing information or documents listed in the Telecommunications Interception and Access Act 1979 Report for the year ending 30 June 2011.

Modernising the ASIO Act 1979

The reforms proposed to the ASIO Act are minor; however it should be noted that ASIO has enjoyed an enormous increase in funding, powers and human resources since 2001 and is an agency protected from public scrutiny. It is provided blanket immunity from Freedom of Information, unlike the CIA or the British intelligence agencies. While oversight is provided by the Inspector-General of Intelligence and Security, that agency is inadequately resourced for its important and large mandate.

It is positive that the IGIS operates independently of government and has broad investigatory powers to investigate complaints and conduct inquiries and regular inspections and monitoring of security and intelligence agencies, however, the agency is under a great deal of pressure to monitor and verify the activities of six agencies, and conduct investigations as requested by the Prime Minister, with just 14 staff.

Many additional provisions under the ASIO Act have never been invoked, leading some commentators to question whether they are in excesses to actual requirements. ASIO's enhanced powers include increased detention powers, secrecy provisions that prevent scrutiny of its questioning and detention powers, and more recently an ability to collect information on Australians in foreign countries if there are supposed impacts Australia's foreign relations. This broadening of the range of matters ASIO can investigate means there is now no need to relate to a security threat.

Proposals the Government is *Considering*

***TIA Act* Single Warrant & Modernising the Industry Assistance Framework**

The Attorney General's paper does not explain how covering 'ancillary service providers' – the many and ever increasing forms of social media – in legislation will address 'current potential vulnerabilities in the interception regime that are capable of being manipulated by criminals'.

The Greens believe it is excessive to extend the reach of surveillance into the retention of all social media exchanges. Does this include all business exchanges on video conferencing platforms?

Recommendation 4: The Committee is encouraged to seek clarification about how the Attorney-General proposes to define ancillary service providers and how the fact that a very limited number are based in Australia and subject to Australian law would be practically addressed.

Bending the Rule of Law for ASIO Officers

The Greens do not believe it is acceptable for ASIO officers to be lawfully entitled to cause harm to persons or property. Given the previously mentioned opacity of ASIO severely limiting public accountability for ASIO's use of ever increasing tax payer resources, ASIO officers are already afforded significant protections.

Giving ASIO the right to disrupt computers could open it to accusations of planting information. Malware used for such purposes can also be designed to benefit non-authorised third parties.

Recommendation 5: The Committee should reject a different standard for ASIO officers and affirm that the highest standards should be stringently adhered to by Australian Government security personnel.

ASIO's Cooperation with the Private Sector

While the Greens are doubtful that the Parliament or public will be provided with information about ASIO's cooperation with the private sector, limits and conditions should indeed be clarified.

ASIO's exchanges with Greens Senators at Estimates demonstrate how difficult it is for the public to actually learn much in this regard. Director General of ASIO Mr. David Irvine said in February 2012 in response to questions about ASIO's use of the National Open Source Intelligence Centre to spy on activists,

> "ASIO may from time to time use external contractors to provide a service that we ourselves would be unable to provide as efficiently and as effectively as we could buy it in. For example, we contract out the compilation of media articles, media monitors and that sort of thing. I guess that is normal practice. But I will not, if you do not mind, go into specific details about outsourcing generally. ..That goes to the sources and methods issue for ASIO, and it is very definitely an operational issue which I could not answer."

Recommendation 6: The Committee should recommend that ASIO is prohibited from outsourcing illegal or untoward activities.

Proposals on which the Government is *expressly seeking the views of the Committee*

The Attorney General's Discussion Paper does not attempt to address the two most controversial proposals on which it seeks the Committee's views – data retention and punishment for refusal to assist in decryption.

Recommendation 7: The Committee should seek the views of the Attorney General as to why she is seeking the views of the Committee on proposals that seemingly do not merit explanation or justification.

Punishment for refusal to assist in Decryption

While the integrity of Australian's right to silence has been damaged by the anti-terrorism laws, with regard to other criminal offences it remains intact. This proposal further degrades the right to silence, presumably to pre-trial investigations and undermines the privilege against self incrimination.

Recommendation 8: The Committee should oppose this proposal as a serious erosion of the legal and human rights of Australians.

Data Retention for up to 2 Years

Data retention is unacceptable and indiscriminate surveillance; treating all citizens as suspects. Retaining all data, for all Australians, for years means that every article read online, detailed locational data collected by phones, every email sent, every item purchased would be captured. 96% of recent Sydney Morning Herald readers poll on the question were opposed.

Courts in Romania, Germany, and the Czech Republic have ruled that national data retention laws based on the 2006 European Data Retention Directive are unconstitutional.

A court in Ireland has referred a data retention case to the European Court of Justice and questioned the legality of the entire EU Data Retention Directive.

It is notable that with regard to data retention, the Attorney General has stated, "I am not yet convinced that the cost and the return - the cost both to industry and the [civil liberties] cost to individuals - that we've made the case for what it is that people use in a way that benefits our national security". If our own Attorney General is not convinced, why should the Australian people submit to such extraordinary surveillance overreach?

The vast amounts of data that would be retained poses a security threat because it would be vulnerable to theft and hacking by unauthorised persons or governments, private entities or criminal actors.

Australians have a strong tradition of standing up for free speech and freedom of association - we need to safeguard these traditions in the online environment.

Recommendation 9: The Committee should reject the data retention proposal outright as impractical, dangerous, and a serious erosion of the legal and human rights of Australians.

Amendments made to the *Telecommunications Interception Act 1979* since 11 September 2001

There have been 45 amendments to the *Telecommunications (Interception and Access) Act 1979* since 11 September 2001. There are also 2 unincorporated amendments from recently passed bills.

The nature of these amendments varies.

National Crime Authority Legislation Amendment Act 2001	135, 2001	1 Oct 2001	Schedules 1–7 and 9–12: 12 Oct 2001 (*see Gazette* 2001, No. S428) Schedule 8: 13 Oct 2001 (*see Gazette* 2001, No. S428) Remainder: Royal Assent	—	Terminology change – “Chairman” to “chair”
Cybercrime Act 2001	161, 2001	1 Oct 2001	21 Dec 2001 (*see Gazette* 2001, No. S529)	—	Consequential amendments to inserting cybercrime provisions into Criminal Code
Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004	127, 2004	31 Aug 2004	(*see* 127, 2004 below)	—	Consequential amendments to inserting cybercrime provisions into Criminal Code

Royal Commissions and Other Legislation Amendment Act 2001	166, 2001	1 Oct 2001	1 Oct 2001	—	*Unclear*; *possible error*
International Criminal Court (Consequential Amendments) Act 2002	42, 2002	27 June 2002	Schedules 1–7: 26 Sept 2002 (*see* s. 2(1) and *Gazette* 2002, No. GN38) Remainder: 28 June 2002	—	Consequential amendments as a result of the establishment of the ICC
Telecommunications Interception Legislation Amendment Act 2002	67, 2002	5 July 2002	Schedule 1 (items 23, 29, 33, 37, 39): 22 June 2000 Remainder: Royal Assent	Sch. 2 (item 46) [*see* Table A]	Consequential amendments relating to the establishment and repeal of state crime commissions; some terminology amendments.
Proceeds of Crime (Consequential Amendments and Transitional Provisions) Act 2002	86, 2002	11 Oct 2002	Ss. 1–3: Royal Assent Remainder: 1 Jan 2003 (*see* s. 2(1) and *Gazette* 2002, No. GN44)	—	Consequential amendments to arising from the new confiscation of assets regime under the *Proceeds of Crime Act 2002.*
Australian Crime Commission Establishment Act 2002	125, 2002	10 Dec 2002	Schedule 2 (items 190–224): 1 Jan 2003 Schedule 3 (item 17): *(r)*	—	Consequential amendments to the establishment of the ACC (former NCA)
Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003	77, 2003	22 July 2003	Schedule 1 (items 28, 29): 23 July 2003	Sch. 1 (item 29) [*see* Table A]	Authorising officers to act under 65(1) of TIA (consequential)

Telecommunications Interception and Other Legislation Amendment Act 2003	113, 2003	12 Nov 2003	Schedule 1: 6 Feb 2004 (*see Gazette* 2004, No. S27) Remainder: Royal Assent	—	Consequential amendments relating to the WA Crime Commission and the people smuggling provisions in the Criminal Code.
Telecommunications (Interception) Amendment Act 2004	55, 2004	27 Apr 2004	28 Apr 2004	—	Definitions relating to publicly listed ASIO numbers, Cybercrime in Criminal Code.
Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004	127, 2004	31 Aug 2004	Schedule 1 (items 25–29, 31): 1 Mar 2005 Schedule 5 (item 9): *(s)*	Sch. 1 (item 31) (am. by 40, 2006, Sch. 1 [item 16]) [*see* Table A]	Insertion of telecommunications offences into criminal code (incl child pornography); amendments relating to data and storage devices; interception definitions.
as amended by					
Telecommunications (Interception) Amendment Act 2006	40, 2006	3 May 2006	Schedule 1 (item 16): (*see* 40, 2006)	—	New offences relating to stored communications; serious contraventions; access by enforcements agencies to stored communication; warranted, ombudsman’s role, civil remedies.
Telecommunications (Interception) Amendment (Stored Communications) Act 2004	148, 2004	14 Dec 2004	15 Dec 2004	—	Consequential amendments relating to cybercrime offences in Criminal Code

Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Act 2005	95, 2005	6 July 2005	Schedule 1: 1 Mar 2005 Schedule 2 (items 1, 2, 9): 17 Dec 2005 (*see* F2005L04095) Schedule 2 (item 4): *(t)* Schedule 2 (item 5): *(t)* Schedule 2 (item 15): 1 June 1980 Remainder: Royal Assent	—	Amendments relating to emergency services, interception by radio communications inspectors, ancillary offences, civil forfeiture, employees of carriers
Criminal Code Amendment (Trafficking in Persons Offences) Act 2005	96, 2005	6 July 2005	Schedules 1 and 2: 3 Aug 2005 Remainder: Royal Assent	—	Consequential amendments relating to people trafficking offences in the Criminal Code
Statute Law Revision Act 2005	100, 2005	6 July 2005	Schedule 1 (items 66–82): Royal Assent	—	Repeal of provisions relating to defunct crime commissions
Intelligence Services Legislation Amendment Act 2005	128, 2005	4 Nov 2005	Schedules 1–8: 2 Dec 2005 Remainder: Royal Assent	—	DG must give a copy of warrant within 3 days to IGIS

Law and Justice Legislation Amendment (Serious Drug Offences and Other Measures) Act 2005	129, 2005	8 Nov 2005	Schedule 1 (items 70–76): 6 Dec 2005	Sch. 1 (items 75, 76) [*see* Table A]	Consequential amendment to serious drugs offences inserted in the Criminal Code
Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005	152, 2005	14 Dec 2005	Schedule 1 (items 3–18): 1 Oct 2006 (*see* F2006L03104) Remainder: Royal Assent	—	Technical amendments relating to Vic Office of police Integrity and stored communications; terminology
Telecommunications (Interception) Amendment Act 2006	40, 2006	3 May 2006	Schedules 1–3: 13 June 2006 (*see* F2006L01623) Schedule 4: 1 July 2006 Schedule 5: 3 Nov 2006 Schedule 6 (items 1, 3): *(u)* Schedule 6 (item 8): *(u)* Remainder: Royal Assent	Sch. 3 (items 6, 10), Sch. 4 (items 31–34) and Sch. 5 (items 19, 25, 29, 34) [*see* Table A]	New offences relating to stored communications; serious contraventions; access by enforcements agencies to stored communication; warranted, ombudsman's role, civil remedies.
as amended by					
Statute Law Revision Act 2007	8, 2007	15 Mar 2007	Schedule 2 (item 15): *(ua)*	—	administrative

Telecommunications (Interception and Access) Amendment Act 2007	177, 2007	28 Sept 2007	Schedule 2 (item 1): (*see* 177, 2007 below)	—	ACMA, cooperation with interception agencies, access to data, use of information, disclosure, authorisation, offences
Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006	86, 2006	30 June 2006	Schedule 1 (items 76–85, 88–92): 30 Dec 2006 (*see* s. 2(1)) Schedule 1 (items 86, 93–95): *(v)* Schedule 1 (items 87, 96): *(v)*	—	Consequential to the establishment of the LEIC
Law and Justice Legislation Amendment (Marking of Plastic Explosives) Act 2007	3, 2007	19 Feb 2007	Schedules 1–3: 25 Aug 2007 Remainder: Royal Assent	—	Consequential to the insertion of Div 101 (Terrorism) in the Criminal Code
Telecommunications (Interception and Access) Amendment Act 2007	177, 2007	28 Sept 2007	Schedule 1: 1 Nov 2007 (*see* F2007L03941) Schedule 2 (item 1): *(w)* Schedule 2 (items 2–26): 29 Sept 2007 Remainder: Royal Assent	Sch. 1 (items 57–59, 63–68) and Sch. 2 (items 22–26) [*see* Table A]	Implementing name change of Act to *Telecommunications (Interception and Access) Act 1979*

Telecommunications (Interception and Access) Amendment Act 2008	23, 2008	26 May 2008	Schedule 1 (items 1–19): 27 May 2008 Schedule 1 (items 20–25, 35, 37, 39A): 1 July 2008 (*see* F2008L02096) Schedule 1 (items 43A, 46A): 1 July 2008 Remainder: Royal Assent	—	Terminology chances relating to telecommunications devices
Telecommunications Interception Legislation Amendment Act 2008	95, 2008	3 Oct 2008	Schedule 2 (items 1–11, 13, 21, 25–27): 4 Oct 2008 Schedule 2 (items 12, 14–20, 22): *(x)* Schedule 2 (items 23, 24): Royal Assent	Sch. 2 (items 25–27) [*see* Table A]	Terminology changes
Telecommunications Interception Legislation Amendment Act (No. 1) 2009	32, 2009	22 May 2009	Schedule 1: 18 June 2009 (*see* s. 2(1)) Schedule 2 (items 2–4): 23 May 2009	Sch. 2 (item 4) [*see* Table A]	Minor administrative changes

Trade Practices Amendment (Cartel Conduct and Other Measures) Act 2009	59, 2009	26 June 2009	Schedule 1 (item 2): 24 July 2009	—	Insertion of serious offences relating to cartel conduct
Telecommunications (Interception and Access) Amendment Act 2010	2, 2010	12 Feb 2010	13 Feb 2010	Sch. 2 (items 14–17) [*see* Table A]	Appropriate use of network (Cth agency), permitted purpose, network protection duties, responsible person for computer network
Crimes Legislation Amendment (Serious and Organised Crime) Act 2010	3, 2010	19 Feb 2010	Schedule 4 (items 14–16, 16A, 17, 18, 18A–18H, 18J): Royal Assent	Sch. 4 (items 18, 18J) [*see* Table A]	Offences involving criminal organisations; use of information for organised crime control law
Crimes Legislation Amendment (Serious and Organised Crime) Act (No. 2) 2010	4, 2010	19 Feb 2010	Schedule 4 (item 4) and Schedule 7 (items 25, 29): 20 Feb 2010	Sch. 7 (item 29) [*see* Table A]	Serious offence is also an offence involving a serious organisation
Statute Law Revision Act 2010	8, 2010	1 Mar 2010	Schedule 1 (items 48–52) and Schedule 5 (item 123): Royal Assent	—	administrative

Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010	42, 2010	14 Apr 2010	Schedule 1 (items 75–78): 15 Apr 2010	Sch. 1 (item 78) [*see* Table A]	Sexual offences against children and offences relating to child pornography
				—	
Trade Practices Amendment (Australian Consumer Law) Act (No. 1) 2010	44, 2010	14 Apr 2010	Schedule 4 (item 2): 1 July 2010		administrative
Anti-People Smuggling and Other Measures Act 2010	50, 2010	31 May 2010	Schedule 1 (items 17, 18) and Schedule 3: 1 June 2010	—	Definition of immigration offence, serious offence, foreign intelligence
Freedom of Information Amendment (Reform) Act 2010	51, 2010	31 May 2010	Schedule 5 (item 76) and Schedule 7: *(y)*	Sch. 7 [*see* Note 1]	Amendments relating to the establishment of the Information Commissioner
Trade Practices Amendment (Australian Consumer Law) Act (No. 2) 2010	103, 2010	13 July 2010	Schedule 6 (items 1, 140): 1 Jan 2011	—	administrative

Corporations Amendment (No. 1) Act 2010	131, 2010	24 Nov 2010	Schedule 1 (item 21): 13 Dec 2010 (*see* F2010L03188)	—	Market misconduct definition
Crimes Legislation Amendment Act 2011	2, 2011	2 Mar 2011	Schedule 1 (items 5–8): Royal Assent	Sch. 1 (items 7, 8) [*see* Table A]	Permitted purpose in relation to the ACC
Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act 2011	3, 2011	2 Mar 2011	Schedule 2 (item 28): 3 Mar 2011	—	administrative
Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011	4, 2011	22 Mar 2011	Schedules 1–5, Schedule 6 (items 28, 29) and Schedule 7: 23 Mar 2011	Sch. 1 (items 28, 29), Sch. 2 (item 9), Sch. 3 (item 9), Sch. 4 (item 4), Sch. 5 (item 37) and Sch. 6 (item 29) [*see* Table A]	Exercise of warrant powers, disclosure of telecommunications data in relation to missing persons, cooperation between intelligence agencies

Acts Interpretation Amendment Act 2011	46, 2011	27 June 2011	Schedule 2 (item 1140) and Schedule 3 (items 10, 11): 27 Dec 2011	Sch. 3 (items 10, 11) [*see* Table A]	Administrative
Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Act 2012	7, 2012	20 Mar 2012	Schedule 3 (items 42–49): [*see* Note 2 and Table A]	Sch. 3 (item 49) [*see* Table A]	Consistency with MACMA, communicating lawfully intercepted information

Amendments made to the *Australian Security Intelligence Organisation Act 1979* since 11 September 2001

Intelligence Services (Consequential Provisions) Act 2001	153, 2001	1 Oct 2001	29 Oct 2001 (*see* s. 2)	S. 4 and Sch. 1 (items 7–9) [*see* Table A]	Provisions relating to the establishment of the PJC on ASIS, ASIO and DSD
Abolition of Compulsory Age Retirement (Statutory Officeholders) Act 2001	159, 2001	1 Oct 2001	29 Oct 2001	Sch. 1 (item 97) [*see* Table A]	administrative
Cybercrime Act 2001	161, 2001	1 Oct 2001	21 Dec 2001 (*see Gazette* 2001, No. S529)	—	Consequential relating to the computer offences in the Code
				—	
Australian Crime Commission Establishment Act 2002	125, 2002	10 Dec 2002	Schedule 2 (items 2–4): 1 Jan 2003		Consequential amendments relating to establishment of ACC (former NCA)
Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003	77, 2003	22 July 2003	Schedule 1: (items 1–8, 15–29): 23 July 2003 Schedule 1 (items 10, 11): *(q)* Remainder:	Sch. 1 (items 5, 11, 20, 27C) [*see* Table A]	Including new powers, definitions and offences relating to searches, terrorism offences, politically motivated violence, seizable items, powers (terrorism), use of forces, powers to remove and retain information, offences for contravention

			Royal Assent		
ASIO Legislation Amendment Act 2003	143, 2003	17 Dec 2003	18 Dec 2003	Sch. 1 (items 2, 4, 6, 11) [*see* Table A]	Time for questioning through interpreter; preventing unauthorised overseas travel by person specified in warrant, Direction by prescribed authority to detain, secrecy relating to warrants and questioning
Communications Legislation Amendment Act (No. 1) 2004	35, 2004	20 Apr 2004	21 Apr 2004	—	Administrative
Anti-terrorism Act (No. 3) 2004	125, 2004	16 Aug 2004	Schedule 2: 13 Sept 2004	Sch. 2 (item 2) [*see* Table A]	Surrender of passport if person is subject of warrant
Australian Security Intelligence Organisation Amendment Act 2004	141, 2004	14 Dec 2004	14 Dec 2004	—	Amendment to prescribed action
				—	
Australian Passports (Transitionals and Consequentials) Act 2005	7, 2005	18 Feb 2005	Ss. 4–11 and Schedule 1: 1 July 2005 (*see* s. 2(1)) Remainder: Royal Assent		Consequential amendments to name change of Passports Act
Telstra (Transition to Full Private Ownership) Act	118, 2005	23 Sept 2005	S. 3: Royal Assent Schedule 1	S. 3 [*see* Table A]	Definition relating to carriage service provider

2005			(items 43–46): 24 Nov 2006 (*see* F2006L03997)		
Intelligence Services Legislation Amendment Act 2005	128, 2005	4 Nov 2005	Schedules 1–8: 2 Dec 2005 Remainder: Royal Assent	—	Giving warrants to IGIS, definitions of intelligence security agencies
Anti-Terrorism Act (No. 2) 2005	144, 2005	14 Dec 2005	Schedule 10 (items 1–25): Royal Assent Schedule 10 (items 26–28): 15 Dec 2005	Sch. 10 (item 25) [*see* Table A]	Prescribed authority, warrants, release of a person under a 34D ASIO warrant, preventative detention, questioning, data devices, retaining aircraft documents
Telecommunications (Interception) Amendment Act 2006	40, 2006	3 May 2006	Schedule 1 (items 13–15): 13 June 2006 (*see* F2006L01623)	—	Administrative and consequential to TIA Act name change
ASIO Legislation Amendment Act 2006	54, 2006	19 June 2006	Schedule 1: 20 June 2006 Schedule 2: *(r)* Remainder: Royal Assent	Sch. 1 (items 16–21) [*see* Table A]	Including: question and detention warrants, interpreter, IGIS present when custody, humane treatment, secrecy
Law Enforcement (AFP Professional Standards and Related Measures)	84, 2006	30 June 2006	Schedule 3A (items 1–9): *(s)* Schedule 3A	—	Administrative

Act 2006			(items 10–22): *(s)*		
Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006	86, 2006	30 June 2006	Schedule 1 (items 6–10): 30 Dec 2006 (*see* s. 2(1))	—	Consequential to the establishment of the LEIC.
Privacy Legislation Amendment (Emergencies and Disasters) Act 2006	148, 2006	6 Dec 2006	7 Dec 2006	—	Designated secrecy provision
Law and Justice Legislation Amendment (Marking of Plastic Explosives) Act 2007	3, 2007	19 Feb 2007	Schedules 1–3: 25 Aug 2007 Remainder: Royal Assent	—	Definition of terrorism offence
Australian Citizenship (Transitionals and Consequentials) Act 2007	21, 2007	15 Mar 2007	Schedules 1–3: 1 July 2007 (*see* s. 2(1) and F2007L01653) Remainder: Royal Assent	—	administrative
Anti-People Smuggling and Other Measures Act 2010	50, 2010	31 May 2010	Schedule 2: 1 June 2010	—	Amendments to definition of security
Telecommunications Interception and Intelligence Services Legislation Amendment Act 2011	4, 2011	22 Mar 2011	Schedule 6 (items 1–17, 29): 23 Mar 2011	Sch. 6 (item 29) [*see* Table A]	Cooperation, assistance and communication between intelligence agencies
Statute Law Revision Act	5, 2011	22 Mar 2011	Schedule 6 (items 10, 11):	—	administrative

2011			19 Apr 2011		
Acts Interpretation Amendment Act 2011	46, 2011	27 June 2011	Schedule 2 (item 242) and Schedule 3 (items 10, 11): 27 Dec 2011	Sch. 3 (items 10, 11) [*see* Table A]	administrative
Intelligence Services Legislation Amendment Act 2011	80, 2011	25 July 2011	Schedule 1 (items 1–18, 29–31): 26 July 2011	Sch. 1 (items 29–31) [*see* Table A]	Foreign intelligence, application provisions, definition of agency head.