Submission to Senate Legal and Constitutional Affairs Standing Committee Inquiry on Comprehensive Revision of Telecommunications (Interception and Access) Act 1979

This submission is based entirely upon publicly available sources.
The list of appendices at the back does not appear in order of mention.
Appendices are accessible via control/click from the text.
Some surveillance programs are not named but shown as eg. A-redact

Contents

I quote from the RSL building in Perth: "They only deserve freedom who are prepared to defend it."

Introduction

As there will be plentiful input from elsewhere on the security and law enforcement aspect of the relevant Australian laws on electronic interception, this submission will focus on the civil liberties and privacy aspect.

It is also worth noting that unlike in the US, sensible public discussion about the broad parameters of surveillance versus individual liberties in Australia and the UK has been very difficult due to an unwillingness by both governments to engage with the public. In the US accountability of the security services to the elected Congress has been compromised by Congress being given false information about bulk surveillance.

Thomas, Hartree and Aiken are among those quoted as saying the world would only ever need a few computers. This failed to see the development of the PC and mobile devices. With Berners-Lee's coupling of the computer with the internet, the stage was set for mass data collection and surveillance or God-like omniscience, centred on Fort Meade and soon Bluffdale, Utah, ironically the US state associated with latter day saints. A closely linked facility sits in Cheltenham in the UK, GCHQ. And there is a new black building in Canberra with similar associations. The US NSA reportedly has access to a large number of sigint stations round the world with up to 50,000 "insertion" points. That is twice the total number of plutonium "pits" (nuclear bomb triggers) the US currently has, as part of another key US form of security, now controlled by the NNSA, the National Nuclear Security Administration.

Sixty seven years to the day after D-Day, it was revealed that that total surveillance state had come to pass. On June 6, 2013, Edward Snowden, an NSA contractor's employee, whistleblew on what appears to be widespread extralegal and extrajudicial surveillance of people anywhere in the world. Snowden may well have been responding to reports that the US President was about to meet his Chinese counterpart in California to lecture him on state sponsored cyber hacking. Some information about an operations HQ in Shanghai for hacking by China had been given in an ABC program earlier in the year. As an aside, the US and China apparently used to have a joint station to spy on Russia in Henan province associated with the PLA University of Foreign Languages.

Edward Snowden's actions had been preceded by a film based around pre optic fibre surveillance. Echelon Conspiracy, inspired by the surveillance system ECHELON, is a 2009 action thriller film directed by Greg Marcks. It tells the story of Max Peterson (Shane West), an American computer specialist who attempts to uncover a secret plot to turn the world into a global police state. After being chased down by NSA agent Raymond Burke (Martin Sheen), Peterson decides to flee to Moscow. See https://en.wikipedia.org/wiki/ECHELON

The primary issue is whether governments, including our own, have the right to collect and analyse information on every individual and organisation, even though that person or organisation is acting lawfully in the way they live their lives or

conduct their business affairs, and there is no suspicion of anything to the contrary. The UN Declaration of Human Rights (1948) supports that view as does Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Such privacy concerns are reflected in the protections of privacy supposedly provided by the acts of Parliament reflected in Appendix 1, Appendix 2, and Appendix 3. Article 19 of the ICCPR re freedom of expression is of little value if people are spied on simply for having values, views or opinions which are expressed peacefully and would be implemented in a way designed to ensure a peaceful change in public policy. People going about lawful activities online or onphone even eg. a Skype conversation with a family member or friend should not have that digital data collected and stored. UN views on the matter have recently been reiterated (see Appendix 9) (it is noted that offices of some ambassadors to the UN have reportedly been tapped by the US). The Carnell IGIS Report on a Mr Parkin some years ago (Appendix 8) was straight out of Kafka in denying Mr Parkin any basis on which to challenge a security assessment, something some refugees in Australia face right now.

Barack Obama had said in 2007 on surveillance:
"I will provide our intelligence and law enforcement agencies with the tools they need to track and take out the terrorists without undermining our Constitution and our freedom. That means no more illegal wiretapping of American citizens. No more national security letters to spy on citizens who are not suspected of a crime. No more tracking citizens who do nothing more than protest a misguided war. No more ignoring the law when it is inconvenient. That is not who we are. And it is not what is necessary to defeat the terrorists. The FISA court works. The separation of powers works. Our Constitution works. We will again set an example for the world that the law is not subject to the whims of stubborn rulers, and that justice is not arbitrary."

Further in 2005 Obama said: "…And if someone wants to know why their own government has decided to go on a fishing expedition through every personal record or private document – through library books they've read and phone calls they've made – this legislation gives people no rights to appeal the need for such a search in a court of law. No judge will hear their plea, no jury will hear their case. This is just plain wrong. Giving law enforcement the tools they need to investigate suspicious activity is one thing – and it's the right thing – but doing it without any real oversight seriously jeopardizes the rights of all Americans and the ideals America stands for." - Barack Obama, Speech on the Senate Floor, December 15".

His actions as President have yet to fully reflect these views.

Australia is part of the Five Eyes (UKUSA) agreement with Canada, New Zealand, the UK, and the US for Anglosphere spying on the themselves and on the rest of the world. The followed the 1943 BRUSA Agreement. A book called *Rooted in Secrecy* by Coxsedge et al outlined some of the abuses of surveillance in Australia up until they were examined by the first Hope Royal Commission in 1974-7. The Samuels and Codd Royal Commission 1994-5 looked at whether ASIS held tens of thousands of files on Australian citizens. This was denied by the Commissioners but the Minister did acknowledge ASIS held files.

It is not possible to consider changes to the Telecommunications Interception Act in isolation; we must consider other key Acts and the Ministerial obligations and

discretions which exist under those Acts (Appendix 2, Appendix 3). We must also consider the sanctions or lack of them for key parties who breach the acts. For instance the Australian Information Commissioner apparently has no power to impose penalties for breaches of privacy.

The following comes from rense, Echelon & Related Data Interception Capabilities 2000. See http://rense.com/general/data.htm
"4. A second area of apparent conflict concerns states' desires to provide communications interception for legitimate law enforcement purposes. The technical and legal processes involved in providing interception for law enforcement purpose differ fundamentally from those used in communications intelligence. Partly because of the lack of parliamentary and public awareness of Comint activities, this distinction is often glossed over, particularly by states that invest heavily in Comint. Any failure to distinguish between legitimate law enforcement interception requirements and interception for clandestine intelligence purposes raises grave issues for civil liberties. A clear boundary between law enforcement and "national security" interception activity is essential to the protection of human rights and fundamental freedoms."

Personally, I understood how easy it was for satellite communications and even copper wire communications to be tapped, as they probably have been for years from places like Pine Gap and Nurrungar, as well as an ASD station in WA's midwest (see report in the Weekend West, http://au.news.yahoo.com/thewest/a/19383004/spy-base-in-our-backyard/). But I wondered about fibre optic cable, until now I realise that governments and their security services have reportedly insisted on communications companies compromising their ethical relationship with their customers by actively splitting the signal stream using beam splitters (eg. the Telstra/Reach STATEROOM operation with the NSA - see Appendix 4), and maybe even capturing particular signals such financial, economic and stock indices and interfering with them before on-sending. A-redact, B-redact and C-redact, D-redact and E-redact as detailed in *Der Spiegel* on 29 th December 2013, would allow this.

Among the EU Parliament LIBE Committee's findings in its draft report of 8th January 2014 (see Appendix 16) were:
"[Information] Points specifically to US NSA intelligence programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of leading US internet companies (PRISM programme), the it analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (F-redact), access to computer and telephone networks and access to location data, as well as to systems of the UK intelligence agency GCHQ such as its upstream surveillance activity (Tempora programme) and decryption programme (G-redact); believes that the existence of programmes of a similar nature, even if on a more limited scale, is likely in other EU countries such as France (DGSE), Germany (BND) and Sweden (FRA)."

In 2008 James Bamford in his book *The Shadow Factory* discussed the splitter which siphons off information from an optic fibre cable. Nicky Hager had also written of it in his book (see Appendix 13) about New Zealand.

It is now clear that deliberately building vulnerabilities into digital telecommunications facilities at the design stage to allow legitimate law enforcement

access was agreed upon through the ILET Seminar at the International Telecommunication Union in the 1990s and one key meeting in 1995 was held in Canberra. The standard was IUR or 1.0 or Enfopol 98 (see Appendix 24), adopted by Australia and other countries including China. So recent allegations of deals in the US by the government to deliberately weaken encryption in eg. security dongles do have a history.

Julie Bishop who is responsible for ASIS, and George Brandis who is responsible for ASIO won't even discuss the policy issues attaching to this debate. Normally lack of discussion of security is limited to operational issues. If there can be no public debate about security policy versus human rights and privacy, then the matter has moved out of democratic control, and so of answerability to the electorate. Julie Bishop's commentary on a visit to the US in late January 2014 was to the effect that Eric Snowden who had called the US Government to account for flouting the US Constitution was a traitor, but apparently not those who had flouted the Constitution.

Under the Five Eyes policy, it is possible that it is unclear to who it is that the Australian, NZ, Canadian and UK security agencies actually answer to.
Forty years ago this year, when ASIS reportedly assisted in the overthrow of a democratically elected government in Chile, followed by the death of President Salvador Allende, and then the Pinochet regime under which people were "disappeared", was ASIS acting with the knowledge or approval of the Whitlam Labor government? Or was ASIS acting on its own based on a link with a foreign government? If so, has that changed in those forty years? A few years ago ASIS apparently lost six agents in Egypt, yet it is not clear what threat Egypt posed to Australia that required the Australian public to pay for ASIS operations in Egypt.

Does our federal government support unrestricted offtake under PRISM by the US NSA of the communications of Australians, and further, referral of that material to Australian agencies? Australians are entitled to know what the policy is. And the policy can't be made by Nick Warner of ASIS, or David Irvine of ASIO, or Dr Paul Taloni in charge of ASD, but by the elected government. There are also suggestions that Australia offered to capture information for other Five Eyes partners which they might not legally have been allowed to capture themselves. See Appendix 42.

The issue of ultimate loyalty to the democratic government of the day came up many years ago when Harold Salisbury was police commissioner in South Australia under Premier Don Dunstan and considered his ultimate duty was to someone other than the elected Premier in regard to the activities of the police special branch.

Very little of the US discussion on the current issues has seemed to be about protections built into surveillance of non-US citizens, although see the December 2013 report to the President, see Appendix 22.

It would be quite easy to circumvent laws in one UKUSA country protecting the privacy of its citizens by having another UKUSA country collect the intelligence and share it, as ASD apparently offered to do in 2008 (see Appendix 41) at a meeting in GCHQ Cheltenham. This possibility has also been recognised in the draft EU Parliament report (Appendix 16).

Programs

Some of the espionage programs are listed here. This does not include the targeted access operations (TAO) programs; see Appendix 17.

Earlier

Echelon
Advanced Rhyolite

Current

Stellar Wind
PRISM
Tempora
Boundless Informant (says it all really about bulk surveillance), using eg. PRISM and Tempora
Stateroom

Operating bases in Australia

The surveillance bases in Australia include:

Kojarena, WA, a "Dictionary" base - see Appendix 26 re a previous keyword list
Wagga, NSW
Pine Gap and Nurrungar, NT

Many of us are familiar with the fate of the Whitlam Labor government in 1975 which had tried to exercise appropriate sovereign participation in control over the central Australian bases.

National legislation on surveillance

The Telecommunications (Interception and Access) Act 1979 must be considered in the context of a number of other acts including the Australian Security Intelligence Organisation Act 1979, the Intelligence Services Act 2001, the Office of National Assessments Act 1977, the Privacy Act 1988, and the Australian Human Rights Commission Act 1986.

Bulk surveillance, warrantless surveillance, targeted access operations, metadata and digital data collection and storage, implanted chips, emanation detection, deliberately insecure encryption, optical beam splitting, nation to nation secret data swaps, website capture and replacement, alterations of data streams, and respective rights of citizens, residents and aliens need to be set against this legislative background.

The Australian Security Intelligence Organisation Act 1979 provides the legislative basis for the work of ASIO.
The Intelligence Services Act 2001 ('the Act') provides the legislative basis for the work of ASIS (primarily humint), DIGO and ASD (primarily comint).

The Telecommunications (Interception and Access) Act 1979 provides for general control of the activities of a number of Australian agencies.
The Office of National Assessments Act 1977 provides for high level security and intelligence integration and assessment.

The Government describes the overarching relationships as follows:

"The Inspector-General of Intelligence and Security provides the independent assurance that AIC agencies conduct their activities within the law, behave with propriety and comply with ministerial guidelines and directives .

The National Security Committee of Cabinet (NSC) is the peak ministerial decision making body on national security matters, and the Secretaries Committee on National Security the peak officials level committee considering national security matters.

The National Intelligence Coordination Committee, chaired by the National Security Adviser, ensures the broad national intelligence effort is fully and effectively integrated.

Parliamentary oversight of the administration and expenditure of the Australian Intelligence Community is the responsibility of the Parliamentary Joint Committee on Intelligence and Security." Ministers are also required to issue directions and guidelines to most of the security agencies. ONA is an exception it seems, but has been given them anyway.

As to the requirements set out in Appendix 2, here are the Minister's Guidelines for ASIO:

http://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf

As to the requirements set out in Appendix 3, here are the Minister's Rules and Guidelines:

http://www.asis.gov.au/Privacy-rules.html

http://www.asd.gov.au/publications/dsdbroadcast/20121002-privacy-rules.htm

http://www.defence.gov.au/digo/library/digo-privacy-rules.pdf

http://www.ona.gov.au/media/10288/privacy-guidelines.pdf

UKUSA and people

New Zealand is a member of the UKUSA Agreement along with the four following agencies:

- Communications Security Establishment Canada (CSEC)
- Australian Signals Directorate (ASD), Australia

- Government Communications Headquarters (GCHQ), United Kingdom
- National Security Agency (NSA), United States

Here are some current key figures who play a part in the Five Eyes arrangement and associated security, human rights and privacy issues. They have in practice considerable discretions which from an accountability perspective, are hard to publicly check. There is a somewhat wider grouping who meet in an IIRAC seminar every couple of years (Appendix 45).

Australia
Dr Margot McCarthy Australian National Security Adviser
David Irvine, ASIO
Nick Warner, ASIS
Dr Paul Taloni, ASD
Tony Negus, AFP
Committee on Intelligence and Security
National Security Committee of Cabinet
(see also Monitoring Agencies below)

Canada
Michel Coulombe Canadian SIS
John Forster, Chief Canadian CSEC
Warren Tucker, Director NZ SIS
(plus monitors)

NZ
Ian Fletcher, Director NZ GCSB

UK
Sir Malcolm Rifkind, Chairman, UK Intelligence and Security Committee (ISC).
Sir Iain Lobban, Director, UK GCHQ (retg)
Andrew Parker, Director General, UK Security Service
Sir John Sawers, Chief, UK Secret Intelligence Service

Andrew Parker, Chief, MI5

Sir Mark Waller, Intelligence Services Commissioner

Sir Anthony May, Interception of Communications Commissioner

Theresa May, Home Secretary

William Hague, Foreign Secretary

US
Susan Rice National Security Adviser,
James Clapper, Director National Intelligence
Vice-Adm. Mike Rogers, Director NSA, Head US CyberCommand
James B. Comey, Director FBI
John O. Brennan, Director CIA

Reggie Walton, head judge Foreign Intelligence Surveillance Court (FISC)

Monitoring agencies in Australia which have an impact on human rights and privacy

In Australia controls on surveillance and surveillance practices include:

Dr Vivienne Thom, Inspector General of Intelligence and Security (IGIS)
Stephen Sedgwick, Public Service Commissioner (APSC)
Tim Pilgrim, Australian Privacy Commissioner (APC)
Prof. John McMillan, Australian Information Commissioner (AIC)
Colin Neave, Ombudsman
Prof. Gillian Triggs (retg.), head AHRC.
Bret Walker SC, Independent National Security Legislation Monitor (INSLM)
Parliamentary Joint Committee on Intelligence and Security (PJCIS)
The Attorney General, Minister for Foreign Affairs and Defence Minister

Queries to our watchdogs

I asked the IGIS Dr Vivienne Thom and the Information Commissioner Tim Pilgrim about their investigations of the issue of bulk warrantless surveillance of Australians. The replies are shown in Appendix 5, Appendix 6 and Appendix 18. Such surveillance is illegal under the three enabling Acts, the IS Act, the ASIO Act and the T (I and A) Act, except in certain defined circumstances involving full ministerial oversight. There are also restrictions on the collection and analysis of communications of non-Australians, particularly if it can affect an Australian. Appendix 7 is included because it looks at intelligence agency accountability and oversight, as it was seen by Philip Flood in investigating how Australia ended up attacking Iraq in 2003.

Appendix 4 shows the correspondence with Telstra about its response to the report that Telstra/Reach allows bulk surveillance access to its overseas cables.

Emanation security

The ASD assists government and private agencies on preventing loss of data due to radiation emanations from their facilities through by issuing a list of approved consultants. See http://www.asd.gov.au/infosec/emsec.htm
This on the other hand could make it harder to employ equipment such as that for L-redact to pick up these emanations.

Legislative protections for citizens

These are set out in national law as well as ultranational legislation, such as the ICCPR which is used as a basis for AHRC decision making.

National law

The Telecommunications (Interception) Act 1979 (See Appendix 1)

SS. 8A, 25A to 26C of the Australian Security Intelligence Organisation Act 1979 (see Appendix 2).
SS. 6, 8-14 and 35 of the Intelligence Services Act 2001 (see Appendix 3).

Ultranational legislation - ICCPR Articles 17 and 19

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

UNHRC General comment 16 on Article 17 (1988)
http://www.refworld.org/docid/453883f922.html

Article 19

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

General Comment 34 by UN HRC on Article 19
http://www2.ohchr.org/english/bodies/hrc/docs/CCPR-C-GC-34.doc

Here is the view from the UNHCR on terrorism and human rights
http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

Ability to interfere with key financial indicators

Part of the reason for access to private data is stated to be to safeguard the economic security of the spying country. If this data can be altered enroute as it could be in the case of key bank indices such as Libor or Euribor (which have already been the subject of recent fraud), because that was deemed to be in the major banks' and hence the nation's interest, what is to stop it happening? Note that the EU Parliament LIBE Committee (Appendix 16) in its visit to the US was unsatisfied about US Treasury answers on access to the SWIFT international money transfer system by US surveillance agencies.

Questionable targets

Some of the questionable targets which were allegedly subject to electronic espionage which has been revealed in the last six months of 2013 include:

Medecins du Monde, an aid organisation
UNICEF
Angela Merkel, Chancellor of Germany
Herawati Kristiani, wife of SBY, the Indonesian President
The Timor Leste Cabinet
The Copenhagen climate change conference (raising the possibility of important agreements being set aside because they were obtained by unfair advantage)
UN HQ
IAEA, Vienna
OPEC

Those in the list above who were spied upon do not appear to be threats to the world, although OPEC has in the past had a sudden economic impact.

Recommendations on the issue from overseas sources

Here are four, one from the US (1), one from the UK(2), several (EU, OECD, NZ, US)(3) and two from Canada(4).

1.
US President's Committee late 2013 Recommendation 14, see Appendix 22.
We recommend that, in the absence of a specific and compelling showing, the US Government should follow the model of the Department of Homeland Security, and apply the Privacy Act of 1974 in the same way to both US persons and non-US persons.

See Appendix 54.

2.
Sir Mark Waller, 2012 UK ISC Report:
"Based on my scrutiny of GCHQ warrants and authorisations, it is my belief that the activity that GCHQ undertakes is carried out under appropriate authorisation and is necessary for GCHQ's statutory purposes. In addition, I have sought, and received, assurances that considerations of the proportionality of any operations includes an

assessment of whether the expected intelligence gained justifies the level of intrusion into privacy. During my December visit I agreed with GCHQ how this privacy element of proportionality could be more clearly set out in the formal submissions for warrants and authorisations."

I note that GCHQ has recently been accused of participation in murder by playing a part in defining targets for US drones. In the court case the judge ruled against finding GCHQ culpable on the grounds that this would criticise the actions of a foreign state, in this case the US. I also note that in late January 2014, Jemima Stratford, QC a lawyer retained to give an opinion, has said that some of the GCHQ activity is probably illegal (Appendix 53).

3.
See Appendix 16 particularly pp. 40-41, Appendix 27 viz. The Privacy Principles, Appendix 39 Pts. 7, 8, 9, Appendix 42 - see changes to TICS Bill, Appendix 43 esp. Openness p.3 and on p.11 "During my December visit I agreed with GCHQ how this privacy element of proportionality could be more clearly set out in the formal submissions for warrants and authorisations", Appendix 44, pp. 17, 19, 20, 21, 23, 26, 35, 36.

Recommendations

1.That the INSLM review the three Australian acts cited in the light of what is now known and develop new legislative proposals, taking into account Australian privacy and civil liberties legislation, and since the UKUSA partner the UK is part of the EU, EU legislation in that category.

2. That as the ICCPR has worldwide coverage, there be no distinction in the legislation in regards to the rights of Australian and non Australians.

3. That legislation requires Australian security authorities not to act in a way which allows cognate agencies to bypass the privacy and civil liberties guarantees of their own countries.

4. That legislation requires our agencies not to cooperate in commercial espionage unless it involves suspected fraud, money laundering or other criminal activities.

5. Give the PJCIS the power to undertake own motion investigations.

6. Act on the Information Commissioner's recently expressed views on extending FOI coverage.

7. Review whether the new Perth Singapore cable contract mandates installation of beam splitters, and if so, whether access to data carried on overseas optic fibre cables in general should be controlled via CALEA type provisions. This would hold any necessary cryptography access methodology in escrow and be subject to stringent access provisions. See Appendix 33 and Appendix 35.

Further appendices

Some more appendices are noted below, which in view provide a useful context in which to consider the correct balance between surveillance and privacy in Australia. They might be considered as the type of thing the Senate committee would produce as part of a discussion paper of the issue. Those not shown here have been mentioned earlier, but some earlier items are retained to include description or comment.

Appendix 8 looks at the inquiry by the IGIS Ian Carnell in 2005 into an adverse security report on a Mr Parkin, which could not, a la Kafka in his book *The Trial*, be accessed by Mr Parkin, a situation quite a number of refugees face here today. The issue here is that Mr Carnell stated that national security (as perceived by the national security bodies), must prevail over the legal principle of natural justice.
Appendix 10 refers to a Christmas 2013 message US whistleblower Edward Snowden gave broadcast on Channel 4.
Appendix 11 gives information on ASD's enabling legislation, accountability and governance.
In Appendix 12 Fred Kaplan of the US Council on Foreign Relations gives details of the answers US Director of National Intelligence James Clapper gave to the US Congress on 12 March 2013 about bulk data collection by the US NSA, with whom Australia has an agreement.
Appendix 14 gives the link to a Wikipedia summary of the warrantless surveillance controversy.
Appendix 15 gives ASIO's mission and values.
Appendix 16 refers to the draft report on bulk surveillance by the LIBE Committee to the EU Parliament on 8 January 2014, rapporteur an MEP for London, Claude Moraes. That democratic parliament is elected by 500m electors, second to India but transnational. A link to the full draft was provided to the Australian Senate Committee on 10 January 2014. This excerpt deals with attempted extraterritorial application of US law.
Appendix 17 gives some indication of some issues involved with targeted access operations (TAOs) by the Five Eyes agencies.
Appendix 19 covers a 2008 view of the IGIS on whistleblowing given to the House of Representatives Standing Committee on Legal and Constitutional Affairs.
Appendix 20 provides information from a BBC report on bulk data collection through project Echelon in places like Menwith Hall, Pine Gap, and Waihopai. Echelon is now possibly superseded by Boundless Informant using the US NSA's PRISM and UK GCHQ's Tempora and Q-redact.
Appendix 21 describes our NZ Five Eyes (UKUSA) partner in its own words. It has reportedly had to apologise for warrantless spying on 85 of its own citizens.
Appendix 22 provides a link to the report of 12 December prepared for the US President on (bulk) warrantless surveillance, to which he responded on 17 January 2014.
Appendix 23 contains the privacy policies of some Australian telecom providers, but these may be affected by participation in the STATEROOM bulk surveillance on overseas cables and by built in vulnerabilities in encryption software designed for use only with a warrant under the International Telecommunication Union IUR 1.0.
Appendix 25 contains some comments on ASIS and privacy from the 2010-11 IGIS Report.

Appendix 26 contains some reported search terms used by the Echelon "Dictionary" interception stations to sort communications for further analysis. While many inclusions appear to be logically connected with national security, some do not. eg. redheads, porno, sex, which seem more consistent with straightforward personal intrusion which could be used to intimidate individuals. And "veggies"???
It is doubtful that a "dictionary" base used to sort wheat from chaff would be needed for warranted targets as opposed to bulk surveillance.
Appendix 27 refers to the privacy guidelines of the OECD of which Australia is a member.
Appendix 28 is about telecoms cooperation in surveillance and a legal challenge to that by the Electronic Frontiers Foundation.
Appendix 29 is about the OECD and the telecoms relationship with the UK GCHQ.
Appendix 30 is about privacy principles and encryption from an Australian barrister
Appendix 31 is about mandatory data retention in the EU.
Appendix 32 gives a timeline on the development of Echelon.
Appendix 33 is from the American Civil Liberties Union about a method developed under the Clinton administration to give access to encrypted data by law enforcement authorities, using passwords held in escrow.
Appendix 34 is about the proposed bipartisan bilateral bill to strike a balance in the US on surveillance.
Appendix 35 is about the act introduced in the US in the nineties to deal with surveillance of digital telephony, the Communications Assistance for Law Enforcement Act.
Appendix 36 is about protecting critical IT infrastructure in Australia from cyberattack.
Appendix 37 is a useful summary as of 2000 of interception capabilities.
Appendix 38 is setting the record straight on some misinformation about the NSA.
Appendix 39 is about the recent report of the US Privacy and Civil Liberties Oversight Board (PCLOB)
Appendix 40 is about Geoffrey Robertson QC's views on the legality of some Australian surveillance.
Appendix 41 is about consideration of unilateral spying by the US NSA on Australia
Appendix 42 is about offers by ASD to share data with overseas agencies and recent NZ amendments in its Telecommunications (Interception Capability and Security) Bill.
Appendix 43 is the 2012 report of the UK Intelligence Services Commissioner, and details his methods of checking on the spy agencies..
Appendix 44 is the full report of the Canadian Security Intelligence Review (SIRC) Committee for 2012-3.
In the summary table at the back it says:" SIRC also recommends that CSIS develop a legal framework outlining acceptable and prohibited activities, including the corresponding levels of approval within and outside the Service."
On Information Sharing in page 17 it says: " Although ministerial direction to CSIS and associated Service policies are designed to prevent the misuse/abuse of information, both from a security and human rights perspective, it is not clear how CSIS can comply with ministerial direction stipulating that caveats must be used when sharing information with domestic and foreign recipients, when SIGINT collection and dissemination functions run contrary to this expectation."
Appendix 45 is a speech in Auckland in 2008 at the International Intelligence Review Agencies Conference about some key principles for a surveillance organisation given

by the Canadian Communications Security Establishment Commissioner, the Honourable Charles D. Gonthier.
Appendix 46 is about collecting personal data by tapping into smartphone apps.
Appendix 47 is about reporter Glenn Greenwald's response to President Obama's response to the late 2013 report of his security review committee. Greenwald has written much about the Snowden information.
Appendix 48 is about the difficulties of debating bulk data collection in the UK such as that done under Q-redact.
Appendix 49 is about withholding documents related to the bulk collection of Americans' data from a transparency lawsuit launched by the American Civil Liberties Union.
Appendix 50 is about President Obama's response in January 2013 to the report of his review committee on bulk surveillance.
Appendix 51 is about whether the US NSA would secretly target UKUSA Five Eyes partner countries.
Appendix 52 is about whether bulk data collection has played an effective role in preventing known terrorist events.
Appendix 53 is about a current legal opinion on UK GCHQ bulk surveillance given to a UK parliamentary committee.
Appendix 54 is about the US DHS Privacy and civil liberties memorandum

Conclusion

I will finish with a quote from Edward Snowden's Christmas message 2013:

"A child born today will grow up with no conception of privacy at all. They'll never know what it means to have a private moment to themselves an unrecorded, unanalysed thought. And that's a problem because privacy matters; privacy is what allows us to determine who we are and who we want to be."

That is unless democratically elected bodies do what they are supposed to do, which is to fully study the issue in consultation with the people who elected them, and take appropriate steps to balance any necessary surveillance for security, economic stability and prevention and detection of crime against privacy, political freedoms free of covert and overt intimidation, and freedom of expression (within publicly agreed limits).

I look forward to the Inquiry formulating an effective legislative response to some of the issues raised.