Submission No 87

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Mark Newton

Inquiry into potential reforms of National Security Legislation

Joint Parliamentary Committee on Intelligence and Security

Mark Newton
August 2012

Mark Newton PO Box 8138 Station Arcade, SA 5000 **T** +61-416-202-223 newton@atdot.dotat.org

How much is too much?

Introduction

I thank the Committee for the opportunity to make this submission.

The Joint Parliamentary Committee on Intelligence and Security (JPCIS) has been tasked with the examination of a set of proposals for reform of Australia's National Security Legislation, specifically relating to amendments to the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Act 1997*, the *Australian Security Intelligence Organisation Act 1979*, and the *Intelligence Services Act 2001*.

At the outset, it is worth noting that one or more of these Acts has been amended at least once during every Parliament convened since the events of September 11 2001, usually under the impetus of some kind of synthesised *faux*-emergency to give a degree of urgency to the proceedings. Amendments are usually passed on the voices with bipartisan support and very little public debate, usually giving law enforcement agencies and intelligence services more or less exactly what they ask for regardless of how poorly they've performed since the last time they came asking for amendments. The measures that have been legislated have universally provided the law enforcement and intelligence communities with more powers, more money and less accountability, rather like a ratchet.

The public rarely have occasion to observe "balance" in these measures.

For example, no matter how badly ASIO is alleged to have behaved in relation to the surveillance, rendition, and interrogation of Mamdouh Habib at the hands of the United States and Egypt, Australian citizens have never had the opportunity to debate reforms to ASIO that would increase public oversight and impose additional accountability measures intended to assure the public that Australia simply isn't a country that condones torture. The Government's cheerful obsequiousness to ASIO leaves us asking ourselves, for the first time, whether Australia tortures political prisoners. We are left to wonder, in a way that we never wondered before.

Australia's actions towards David Hicks raise similar questions. The assistance provided by the Australian intelligence community to the United States was unable to produce evidence capable of securing a guilty verdict that would be recognized by an Australian court. Australia's Government at the time believed he was guilty; So, were the intelligence services who helped the Government arrive at that belief simply wrong, or were they so blisteringly incompetent that they couldn't prove their case even despite having a suspect in custody, interrogation powers limited only by their likelihood of killing the suspect, and no requirement to honour the usual judicial rules of evidence? And why would we keep listening to people who are either wrong or incompetent when they tell us about the additional powers they need to "reform" their legislative landscape?

The outrageous inappropriate behaviour of the law enforcement community during the Mohammad Haneef affair raise the same questions again. The Clarke Inquiry commissioned by Attorney-General Robert McClelland at least tried to answer some of them. The Inquiry's report concluded that the evidence against Mr. Haneef was "completely deficient"; that the persecution of Mr. Haneef was allowed to continue even though ASIO reported two days after his arrest that there was no information that he was guilty of anything; that AFP domestic counter-terrorism manager Commander Ramzi Jabbour lost objectivity and was "unable to see that the evidence he regarded as incriminating in fact amounted to very little." Yet despite this documented tale of catastrophic incompetence that ran through the AFP, through Cabinet, and right up to the Attorney-General and the Immigration Minister, no legislation has ever been imposed to reform the AFP's procedures, behaviours, and

limitations to ensure that it cannot happen again. Commissioner Mick Keelty was even allowed to resign in dignity without answering for the corruption that had (and, for all we know, still has) infected his organisation.

Balance is required, yet do not see it from this Parliament, or from any other Parliament since the ramp-up of our National Security capabilities hastily began in 2001.

The basic principles upon which democratic government is founded require checks, balances, accountability. Citizens are not supposed to need to trust the government; Indeed, it is our duty to assume that the government is doing its job poorly, and apply pressure to our elected representatives to either rectify lapses or to produce documentation to show that lapses are not happening.

We know that law enforcement and intelligence services need a special kind of scrutiny, because they require a certain amount of secrecy to do their job. But we also know that if we allow the leash to become too loose, they will use our inattention to abuse our trust.

We see this time and time again. Every state police force in Australia has, at some stage during my lifetime, been the subject of a Royal Commission or a judicial inquiry into systemic corruption. Laws are misused in ways abusive to the public, such as when the New South Wales police used their new "consorting" laws, intended to target organized crime, to harrass and persecute an intellectually disabled man in Inverell, eagerly cheered-on by the New South Wales Attorney-General. ASIO has been compromised by foreign spies on many occasions -- most recently this year, when Philip Dorling reported in the Sydney Morning Herald that Canadian spy Jeffrey Delisle was selling vast quantities of Australian highly classified information to Russian agents. Although we give these organisations extensive powers, we know from bitter experience that they cannot be trusted.

We create these organisations and vest them with considerable powers to protect our society. Yet they also provide us with a paradox, in that we know they will abuse the powers we give them, and through that abuse they will themselves become threats to our society.

A corrupt police agency is a threat to the rule of law. An ASIO with unchecked surveillance power is a threat to national security.

It is my belief that our democracy demands that our National Security legislative framework must be resilient in the face of institutional bad actors. When considering policy, the legislator should always be posing the question, "How will this capability be used on a future day when the AFP is as corrupt as Sir Joh Bjelke-Petersen's Queensland Police Force?" or, "What will be the effect on the carriage of justice if this legislated capability is used by police in a manner different to what I expect?" To behave otherwise is to design "brittle" systems of law, which teeter along indefinitely as long as everything goes to plan, but which collapse into society-damaging injustice as soon as they encounter mendacity.

The Discussion Paper

In July 2012, the Attorney General released a discussion paper entitled *Equipping Australia against emerging and evolving threats.*

The paper presented itself as a discussion of "holistic reform" of our National Security Legislation, aiming to "modernise" and "streamline" it to address new "threats to our wellbeing" by means of a package of proposed legislative amendments.

I would like to take issue with the tone and timbre of the document before addressing individual proposals.

To begin with, the discussion paper's representation of "holistic reform" is faulty. To my mind, it is only possible to carry out a "holistic" analysis by considering the entire landscape, *and taking in all relevant views,* before drawing conclusions. The discussion paper cannot possibly make any "holistic" claims because it has only considered the views of the law enforcement and national security communities. We citizens are stakeholders in this too, and frankly this Committee Inquiry is the first occasion I can remember being asked about any of this since 2001.

The document is a wish-list of proposals that have been floating around police forces and Attorney-General's Department bureaucrats for years. Indeed, the Data Retention proposal discussed herein dates back to the Howard Government.

Every now and then these proposals quietly pop up like trial balloons, their proposers judge that the winds aren't blowing in the right direction, and they pop down again until the next opportunity to try them on. It's almost as if the proposals' owners float them every time we swear-in a new Attorney General, just to see if he or she is credulous enough to give them a permissive hearing.

To the credit of our previous Attorneys General, the more contentious proposals detailed in the Discussion Paper have been unable to advance. But that doesn't mean that they've gone away. The Department has a longer memory than any of its Ministers, and can rely on the amnesiac effect of the "brain transplant" they receive whenever there's a change of government or a front bench reshuffle.

The current Attorney General should be praised for bringing these proposals out into the open. Not only are they now receiving the widespread public scrutiny that they've previously been denied, but future Attorneys General will no longer be ignorant of history when they are sworn in, and will be less susceptible to manipulation from their departmental staff.

The Discussion Paper also purports to offer to "modernise" and "streamline" our National Security Legislation. That's a curious notion, suggesting that somehow the *status quo* is a rusty cobwebbed artifact that's no longer capable of performing its intended task.

In truth, it's difficult to imagine any laws that have been updated more often during the 21st century than our National Security Legislation. The *Telecommunications (Interception and Access) Act 1979* in particular has been updated almost every year for a decade; I find it inconceivable that the amendments made earlier this year under the *Telecommunications Interception and Other Legislation Amendment (State Bodies) Bill 2012* are in dire need of modernisation, or that that ASIO is somehow historically constrained by the amendments made to its controlling legislation in response to Wikileaks less than two years ago.

To make a case that a law is too old to be useful, it is first necessary to allow it to become old.

"Streamlining" is another curious target for National Security Legislation. It should always be understood that these laws empower police to gather evidence that will be used to overcome a presumption of innocence in a criminal trial. *It is not supposed to be easy to carry that burden.* As a citizen, I not only know that it's very difficult for police to do their job, I fully expect that the fundamentals of our society are designed to keep it difficult.

Consider the matter in the abstract:

We all know that it's be trivially simple for police to prosecute all manner of crimes if (for example) we maintained police-controlled audio-visual recording equipment in every room of our house. But we don't do that, even though the technology to do it now exists: Making life easy for police is clearly not the number one priority of our society and culture; we all know that in a contest between (for example) the needs of law enforcement and our privacy within our home, law enforcement will ordinarily lose.

As a society, we *know* there is tension between the needs of intelligence and law enforcement and the needs of everyone else. We weigh the balance, and construct strict, limited portals by which government agencies can peer into our lives. Warrant requirements, permits, different rules for free citizens versus prisoners. These are all ways in which society says to law enforcement, "You may go here, but no further."

Not all societies function in that way. We have a term for societies in which the police set the rules of engagement and can conduct themselves as they see fit regardless of the wishes of the polity. We call them, "Police states."

Australia is not a police state. We accept that our intelligence and law enforcement officers must remain within limits, and that exceeding their authority is a form of corruption. We accept that law-abiding citizens confronted with a law enforcement officer demanding information may, in almost all circumstances, simply reply with, "No."

So having established that we are not a police state, the debate then turns to the limitations, the locations of the lines which a policeman may not cross.

In Australia, we have typically set those lines very conservatively. We accept that law abiding citizens should be able to go about their lives without interference *or detailed scrutiny* from the police, and that some kind of immediate need (often accompanied by judicial review) must be demonstrated before a citizen can be hauled into our criminal justice system.

In that sense, National Security Legislation is not supposed to be "streamlined." Although it's no doubt annoying and time consuming for law enforcement officers, the difficulty involved in getting a warrant, and the need to refresh it before its in-built expiry date, is not an "inefficiency." It's a feature, not a bug. It's one of the ways in which Australia has chosen to protect itself from the abusive, corrupt law enforcement agencies that our historical litany of judicial inquiries and Royal Commissions has warned us to expect.

I do not want to be part of a society in which a citizen's communication records (much less their actual communications content) can be delivered to government agents upon invocation of an administrative process. I prefer a society in which it is so difficult for police to obtain unimpeachable evidence that there is no question about whether a convicted defendant is guilty "beyond reasonable doubt." The threat of evidence being disallowed under a "technicality" makes police work harder to build more convincing cases; or it makes them not prosecute defendants in the first place if there's any doubt as to their guilt. Both alternatives strengthen our national security.

For the remainder of this submission, I will address specific elements of the Discussion Paper.

Disagreement with a specific proposal doesn't necessarily imply that I disagree with the problem statements which the Discussion Paper has used to justify the proposal. We live in a world where there are multiple solutions to any given problem, yet this Discussion Paper only provides one response to each of the issues it has raised, the alternative that maximises the benefit to law enforcement. There is no "balance" in these proposals, but there inevitably will be in different proposals designed to address the same problems following consultation with stakeholders outside the law enforcement community.

The Discussion Paper's proposals have also been developed in an absence of quality information. For example, in an interview given to ZDNet on July 29th 2012, AFP Assistant Commissioner Neil Gaughan said, "In the 2010-2011 financial year in excess of 2400 arrests were made through lawful interception alone." When the interviewer introduced the fact that over a quarter of a million telecommunications record requests were made during that year, Mr. Gaughan said, "A lot of time, as with lawful interception, once we provide the evidence that we have to the criminal, we get a conviction without being tested," because the suspect pleads guilty. "So it's really hard to say that 250,000 requests for telecommunications data didn't lead to a significant number of prosecutions."

To which I'd ask: "Why is it hard?" Why isn't the AFP maintaining statistics about that information?

More generally: How can they come before this Committee requesting additional powers without providing any quantitative evidence that their existing powers are insufficient? It seems all we're really left with is "ticking time bomb" movie-plot scenarios.

Mr. Gaughan ended the interview by explaining that his nightmare scenario was "... that there's a piece of information out there that could potentially stop a terrorist act from happening in Australia. If I don't have that information, I can't stop that terrorist attack."

WIth all due respect to Mr. Gaughan, our National Security policies ought not be calibrated to accommodate the fears of whomever has the most exaggerated imagination. Our national security community has never made any effort to convince us that we've ever been under any credible threat of any kind of nation-busting terrorist attack. If after all this time and with all their investigatory powers the best they can come up with is hypotheticals, then what value are we getting from all the money and power we've invested in them?

The Discussion Paper has similar limitations. It alludes obliquely to the Benbrika Group when it discusses the manner in which telecommunications interception has produced prosecutions, but it fails to provide any examples whatsoever of cases in which lack of telecommunications interception has caused prosecutions to fail. The Discussion Paper reads like an account justifying the existence of the *current* repertoire of facilities available to law enforcement and intelligence services, but neglects to make the case for the *extra* facilities it describes.

I find this odd: That in such a voluminous document, with so many proposals for extra power, not one single example has been provided of a case where existing powers are insufficient.

Interception and the TIA Act

Section 1.1 of the Discussion Paper reads like a cheerleading account of the success of the current regime, which seems to be delivering thousands of arrests and thousands of prosecutions for not very much money. It's difficult to consider that many changes to the TIA Act are needed if those numbers are accurate, especially when the discussion paper also says the figures "... may underestimate the effectiveness of interception."

The paper finds it necessary to gloss over the "several men who faced trial in Melbourne" for terrorism in 2008. I find that that's because allegations of terrorism in Australia have historically been so farcical or trivial that they're difficult to take seriously. The case cited by the Discussion paper is that of the Benbrika Group, who certainly made a lot of intercepted phone calls but didn't seem to have any actual targets (they were said to have planned attacks on football games, the Grand Prix, the Crown Casino or maybe John Howard, but hadn't decided at the time of their arrest; their general level of incompetence ought to suggest that they'd be more likely to harm themselves than any hypothetical targets). I'm glad they were apprehended, in the same way I'm glad when any nutcase is apprehended, but it's difficult to consider them to be credible "terrorists" without doing violence to the normal English language meaning of the word, and I believe Benbrika's 15 year sentence was unduly harsh for a conspiracy to plan an act they had no conceivable likelihood of ever carrying out.

More succinctly: Australia's anti-terrorism laws seem to be remarkably good at imprisoning people who harbour antisocial thoughts, but wholly unsuccessful at apprehending people who are credibly likely to damage Australia's national security.

But that's the best we've got? With all the money, power, legislative engineering and manpower we've thrown at our intelligence services since 2001, that's their crowning achievement?

In relation to organized crime: The Discussion Paper has lots of dubious scary numbers (organized crime costs Australia $15b per year? That's the cost of a new iPhone every year for every man, woman and child in Australia, and it's not passing the sniff test, I'm afraid). Then it talks about how broadband internet "has the potential to increase high-tech crime." Well -- Is it? Don't tell me about potential; We've had pervasive broadband throughout Australia for ten years now, it's not something over the horizon anymore. We spend billions of dollars annually on our law enforcement agencies, I expect them to tell us definitively whether broadband *actually does* increase high-tech crime threats in Australia. Don't talk about hypotheticals when trying to justify real-world legislative power-grabs that cause a real-world reduction in the liberties of law-abiding citizens. Not good enough.

I'm not persuaded by claims that the "magnitude of change to the telecommunications environment" has made law enforcement and intelligence gathering difficult. As someone who has worked for an extended period at a large telco and has been involved in telecommunications interception on behalf of law enforcement agencies, it's clear to me that the "change to the telecommunications environment" hasn't been as rapid as the discussion paper makes out, it has evolved over several decades, while the TIA Act has been updated progressively to keep up.

We don't have a problem with interception capabilities in the current telecommunications environment; We have a problem with law enforcement agents thinking in 1980's terms, failing on a personal level to keep up with the changes the world is imposing on the investigatory techniques they're choosing to use.

In Australia, today, every single phone call can be lawfully intercepted, whether it's on a landline or a mobile device. Every broadband session can be lawfully intercepted. Every mobile telephone user can be GPS-tracked. Skype has reengineered their platform to make it more amenable to law enforcement requests for call audio streams, which they are alleged to

provide without the need for a warrant. Social networking sites routinely throw their privacy policies out the window in response to a polite request from law enforcement. Server logs count as business records that can be lawfully subpoenaed or subjected to search warrants.

It is difficult to conceive of a telecommunications environment which is more carefully attuned to the needs of law enforcement -- If only they go through the correct channels and obtain the correct paperwork first.

Many of the proposals in this Discussion Paper are concerned with widening the channels and doing away with the paperwork requirements. These are important safeguards which protect tens of millions of law abiding citizens from law enforcement overreach, allowing them to live their lives without being harassed by the police. They should be non-negotiable, yet here we are...

In its **Access to communications content and communications data** section, the Discussion Paper describes a relatively disordered view of the interaction between ISPs and internet applications. Outside of Government, companies such as Google, Facebook or webmail application operators are not generally described as “service providers.” That term is reserved for ISPs and carriers; Using it to refer to higher-level application operators builds confusing double-meaning into the nomenclature, so one can never make sense of which entity to which the term “service provider” applies.

It’s surprising that the Discussion Paper would make such an error, given that law enforcement and intelligence agencies have been working with Internet technologies for the best part of two decades, and ought to be relative experts by now.

To clarify for the benefit of the Committee:

An ISP has a very simple role in life: It receives “packets” from end users, examines their numeric destination address, and tries to forward them closer to their destination. By analogy, an ISP is like a post office: Envelopes come in from post users, the post office inspects the address on the front, and makes a decision about which ship, truck or plane onto which each envelope should be loaded.

ISPs connect to each other as well as to end users, similar to the way in which mail sorting centres, post agency outlets, and commercial parcel delivery services send envelopes to each other. Global cross-jurisdictional networks are thus formed.

Some of the end users connected to ISPs happen to be companies providing applications to the public. Similarly, some of the end users who send and receive envelopes through the postal network are companies providing applications to the public. Both networks enable commerce, communication, enterprise and innovation.

One can consider a bricks-and-mortar company offering research services by mail -- You could send it a form in an envelope specifying your interest in information about “cat pictures,” and it could send you back another envelope containing a catalogue of the names and addresses of other people who know about cat pictures, so that you can send them letters asking for examples of what they have to offer. We might call this research company, “GooglePost.”

The typical online shop is nothing more than an online analogue to a mail order company.

The point is that we’ve seen all this before. The way in which the internet works is almost exactly the same as the way the postal system works: Services accessible to the public layered on top of a common global substrate that does nothing more than point-to-point delivery.

Law enforcement and intelligence services have known how to run communications interceptions on the postal network for centuries, yet for some reason they become befuddled and confused when they encounter the internet.

My observation is that the confusion arises because they want it to be like a telephone. But it isn’t. It’s like the postal service.

Our society has expectations and norms around law enforcement access to the post. To the extent that those expectations and norms are translatable via analogy to the Internet, I think most people would find them unobjectionable. The concept of communications privacy is key, which means the government should not be able to hoover-up vast quantities of data about

Australian telecommunications users *just in case* a crime happens to be committed. We would never allow that on our postal networks; I can't see any reason why we should on our data networks.

Matters the Government wishes to progress

Examining the legislation's privacy protection objective, the proportionality test for issuing warrants, mandatory record-keeping standards, and oversight arrangements by the Commonwealth and State Ombudsman
I have no objection to examining these items, with a view towards strengthening all of them.

Reducing the number of agencies eligible to access communications information
I support this proposal. In 2010-2011 there were over a quarter of a million requests for telecommunications data, from Government agencies ranging from police forces to local councils. Nobody has any clear knowledge of the pretext for most of those requests, or the legitimacy in making them.

It is unclear to me why records that a conversation has been made aren't treated as sensitively as the content of the communication itself. The data retention scheme proposed by the Discussion Paper seems to be based on an assumption that Australians require their communications content to be well protected but are happy to have records concerning where, when, and to whom they have spoken maintained in a state able to be audited by police. I see no evidence whatsoever that the public agrees with that view. On the contrary, I see mounting public concern about the availability of tracking data every time a new Facebook or Google privacy scandal hits the headlines.

I would consequently support reform to the TIA Act which made it clear that telecommunications data must be afforded the same protection as communications content.

In the interim, the Government ought to commission research to ascertain the views of the public concerning their expectations of telecommunications data privacy. For example, given that communications data maintained by mobile telephone carriers includes GPS location, are Australian citizens comfortable with high-resolution logs of their movements being made available to law enforcement on-demand without a warrant?

Standardising warrant tests and thresholds
The Discussion Paper calls it "standardising," while the analysis text makes it perfectly clear that it really means, "reducing." I do not support this proposal: To law enforcement agencies, high thresholds and detailed tests for warrants is an inconvenience; for the law abiding public, the are important safeguards.

Simplifying the information sharing provisions that allow agencies to cooperate
The Discussion Paper is vague about what this "simplification" would entail, with only a single paragraph at the bottom of page 25 to explain it. I would support simplified sharing between agencies, but only if there is no net reduction in the privacy and due process protections afforded to the public.

In particular, I would not support a sharing regime which enabled an agency which had obtained evidence for a certain purpose to divulge it to a second agency for a different purpose, if that second agency would otherwise be required to obtain their own warrant.

Removing legislative duplication
To the extent that such amendments would be purely administrative or clerical, I would support them.

Aligning industry interception assistance with industry regulatory policy
It is difficult to address this proposal because the Discussion Paper is vague about its meaning.

Clarifying the ACMA's regulatory and enforcement role
The Discussion Paper points out that ACMA rarely uses its powers in relation to the TIA Act because the only effective remedy in its arsenal is court action, which is usually inappropriate.

The Discussion Paper then suggests strengthening ACMA's role by means of additional powers.

I can understand that bureaucrats think that way; Adding powers to bureaucracies is always a good thing if the size of your staff and budget is related to the number of regulatory functions you oversee. But that doesn't make a lot of sense to this taxpayer.

The TIA Act was enacted in 1979. If the ACMA (and its predecessors) have had a power for over 30 years which they've rarely exercised, and which if exercised is usually inappropriate anyway, that strikes me as an excellent reason to abolish the power as part of the regulatory reform process.

Thus, I support "clarifying" the ACMA's regulatory and enforcement role by amending the Act to remove the ACMA from the interception regime.

Matters the Government is considering

Creating a single warrant with multiple TI powers

To the extent that creating this instrument would largely be a paperwork exercise, in that it replaces several largely identical documents with a single document, I support it. If it reduces the applicant's burden of justifying the warrant to a judge in any way at all, I oppose it.

The applicant's requirement to show cause is an important protection to the public, which must be preserved and, where possible, enhanced.

Implementing detailed requirements for industry interception obligations

The Discussion Paper has failed to provide examples of cases which have been unable to proceed, or interceptions which have been unobtainable, due to the workings of the current regime.

When a government issues "detailed requirements," I can tell you exactly how cost-sensitive companies approach them: They implement the bare minimum they can possibly get away with. That inspires the Government to issue requirements that are so expansive and comprehensive that they cover every eventuality, which are so expensive to implement that industry can't do it.

The current industry interception obligations are more consultative. They are able to be "tuned" to meet the circumstances and capabilities of each carrier. They may be messy but they seem to work, despite the drum-beating in the Discussion Paper. I see no reason to proceed with this proposal.

Extending the regulatory regime to ancillary service providers not currently covered by the legislation

The Discussion Paper defines "ancillary service provider" in vague terms, as "Telecommunications industry participants who are not carriers or carriage service providers."

The confused depiction of the modern telecommunications landscape described above strongly suggests that "ancillary service providers" are intended to mean companies such as Google, Facebook, *etc.*

I strongly oppose any move to include those companies into the telecommunications interception regime. Fundamentally, *they are not telecommunications industry participants* by any measure other than the poorly-drawn picture of the Internet presented in this discussion paper.

I can leave feedback on someone's eBay profile in a manner similar to the way I could write on their Facebook wall. Does that make eBay, a supervisor of auctions, an "ancillary service provider," under the authority of the TIA Act?

It strikes me that the law enforcement community would like anybody who maintains any data about anyone to count as an "ancillary service provider," so they can receive intercept warrants (and, presumably, participate in data retention schemes). That view is not acceptable in our society. We don't do it on the postal network, we shouldn't do it on the internet network either.

Given that the overwhelming majority of these companies are offshore anyway, it's difficult to see how Australian interception warrants will be enforceable on them anyway. Even if enacted, the proposal is doomed to failure.

Implementing a three-tiered industry participation model

This proposal is unnecessary, on the grounds that we have it by *fiat* already. Current industry interception obligations are consultative, and the Attorney-General's Department doesn't bother to consult with providers that this proposal would envisage as "tier 3." I believe considering this proposal is a waste of time, and I don't support it.

Matters on which the Government expressly seeks the views of the Committee

Expanding the basis of interception activities

The Discussion Paper is vague about the particulars of this proposal; Specifically which aspects of the discussion relate to the concept of "expanding the basis of interception activities."

My natural inclination is to resist any suggestion of measures to expand the current scope of interception activities.

Establishing an offence for failure to assist in the decryption of communications

The Discussion paper significantly provides no justification whatsoever for this proposal.

I oppose it totally.

There are several reasons for my opposition. The most practical one concerns the inability for law enforcement to distinguish between "failure to assist" and "incapability to provide assistance." How would this proposal avoid the prospect of punishing innocent people for not knowing a password when the police have insisted they do?

I also oppose it due to the way this proposal "dovetails" with other proposals in the Discussion Paper. Consider for a moment how the Queensland Police Commissioner under Sir Joh Bjelke-Petersen, Terry Lewis, would have approached a regime which allowed him to permit police intelligence agents to break laws, to legally insert encrypted data onto a person's computer, then charge him with the offense of failing to assist in its decryption.

Part of a society's National Security is its inherent protection from institutional corruption. These measures open the gate too wide, invite too much abuse, especially in a country where law enforcement corruption has historically been so much more common than terrorism.

Instituting industry response timelines

Analysis of this measure is not provided by the discussion paper, so its meaning is unclear.

Data retention measures

I oppose these proposals outright.

Data retention significantly changes the relationship between the citizenry and the Government, by inviting law enforcement agents into virtually every human interaction.

We would not tolerate this in any offline context. The Government ought to be ashamed of itself for having so little regard for democratic principles that it would even begin to discuss tolerating it online.

Data retention measures make our society less secure, by creating enormous silos of identifiable information in readily attackable locations. One single security breach risks losing everything, on a scale that leaves the United States' experience with Wikileaks in the shade. It is contemptible that the Government has learned no lessons from its own Wikileaks exposure, and still believes that concentrating large troves of leakable, attackable private data is a good idea.

Data retention is inordinately expensive. ISPs will not be able to slip down to their local PC shop and buy $100 hard drives; To be of any use, the data would need to be retained to a standard that would qualify for submission as evidence in a criminal trial. That means audit trails, security classifications, extreme reliability and availability standards, backups, access control, physical security, maintenance contracts, and endless vendor hardware refresh cycles to keep scaling the repository as the volume of data grows. No ISP is ever going to want to be in the media's sights as the organization who let the pedophile go free by accidentally deleting the evidence, so the magnitude of money and effort that'd go into maintaining the integrity of the data store would be extreme.

The Attorney General's Department knows all of this from its industry consultations in 2010, where it asked ISPs for cost estimates; but it seems to have forgotten, and resurrected the proposal anyway.

Data retention is extremely wasteful. The expense described above would be incurred by every ISP targeted by the scheme, acting as a tax on businesses, increasing the cost of telecommunications even as the National Broadband Network promises to reduce it. Massive quantities of money would be spent across the industry to gather dossiers on every Australian telecommunications user, even though barely any of them would ever become subject to a criminal investigation.

The law enforcement community would achieve investigative convenience; but only by outsourcing its evidence-gathering expenses to the telecommunications industry, massively inflating them with inefficiency and duplication, and creating significant new security threats against every Australian citizen unfortunate enough to have data held therein.

And despite all the expense, all the waste, and all the new security vulnerabilities, we'd never be able to seriously trust it, because we'd never be able to be sure that an attacker hadn't already compromised its security measures and used their unauthorized access to insert or alter fraudulent evidence; or that a political party hadn't authorized ASIO to slurp up all the communications and financial records of their political opponents. Don't just think about how it'll be used, think also about how it'll be misused, with 1980's Queensland as the benchmark.

The proposal has been bouncing up and down every now and then for years. This Committee should take the opportunity to finally hammer a stake through its heart. We know better than this.

Telecommunications Security Sector Reform

The Discussion Paper describes the current Telecommunications Security regulatory landscape, and makes some proposals for alternative approaches.

The Analysis section says, "... there is a lack of awareness of national security risks in business decisions by many C/CSPs, which means engagement often occurs late in the decision making process."

Not to put to fine a point on it, that's how our society is supposed to work. It isn't the role of C/CSPs to make business decisions in the intelligence community's best interests (cf: earlier comments about the term "police state"). It's the intelligence community's job to stay sufficiently informed and organizationally nimble that they can accommodate C/CSP business decisions without feeling a need to interfere in them.

The Analysis continues, "Government is concerned that the telecommunications industry is not fully informed about national security risks..." One could argue that the the intelligence community's obsessive focus on secrecy is the root cause of that misalignment, and if they think the telecommunications industry needs to be informed about something then they should... inform them.

The proposed approach involves "an industry-wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference," which they do to the best of their ability already.

There is also a suggested requirement for C/CSPs "to provide Government, when requested, with information to assist in the assessment of national security risks to telecommunications infrastructure." Again, to an extent that already happens; But businesses also need to be mindful of the fact that any information they provide to the Government can potentially be released (e.g., under FOI, subpoena, or leak), so it's wise to be reluctant about sharing.

The preceding two paragraphs perhaps make plain my reaction to the third proposal, "powers of direction and a penalty regime to encourage compliance." Might be considered unnecessarily heavy-handed given the subject matter and the companies involved?

Let us be clear here: The particular business decisions the Discussion Paper takes issue with are those concerning the introduction of new products and services to the Australian communications marketplace. The law enforcement community would like all new products to be designed to be easily wiretapped, which means Australian carriers have traditionally avoided the implementation of encryption on behalf of their customers.

It needs to be understood that this deference to the stated needs of the law enforcement community in relation to encryption and interception creates security risks for Australian telecommunications users, i.e., all of us. Far from requiring C/CSPs to consult with the Government prior to taking business decisions, the law enforcement community should be required to make a case to justify their existing powers, and the risk they present to 22 million lawful Australian carriage service users.

It must also be said that it's very difficult to take seriously the proposal of a penalty on C/CSPs "where a breach has occurred, for example a CSP's data is accessed and published," in the same paper that proposes maintaining vast repositories of otherwise deletable data in attractively attackable Data Retention repositories.

Australian Intelligence Community Legislation Reform

This section in the discussion paper has been organized into sections corresponding to the Government's desire to progress individual proposals.

Matters the Government wishes to progress

Modernise and streamline ASIO's warrant provisions

I strongly object to these proposals.

As I discussed in my introduction, the fact that we are not a police state means that we entertain vigorous debate over the locations of lines-in-the-sand which our police and intelligence agencies may not cross.

As I also discussed in my introduction, those lines have been subject to amendment a great many times over the last decade. With the exception of this current Committee's deliberations, virtually all of the previous amendments to National Security Legislation have been made without public comment or consultation. How did the Governments involved know where the public wanted the lines to be drawn?

Until I hear news of a criminal who "got off" because the authorities were unable to search his computer, I will not accept that references to "computer" in section 25A represent an impediment to law enforcement's operations significant enough to warrant the consumption of this Committee's time.

The requirement for a new warrant in any instance where there is a change in circumstances is an important protection for innocent members of the public built in to the foundation of our criminal justice system; It should not be watered down for ASIO's mere convenience. It is appropriate for ASIO-specific warrants to be more onerous than "regular" warrants due to the deficiencies in public oversight created by ASIO's secrecy.

I do not support an increase in the duration of an ASIO search warrant. I would support a light-weight renewal process for an expired 90 day warrant that would add an extra 90 days without the full burden of obtaining a new warrant, as long as the renewal involved judicial review.

I do not support a renewal process for any warrant older than 6 months. The fact that ASIO must presently restate its intelligence case and reassess the legislative threshold at 6 monthly intervals to replace expired warrants is an important public safeguard, which goes some way towards making up for the loss of checks and balances we'd otherwise have if ASIO wasn't a secret organisation.

Modernise the ASIO Act employment provisions

I have no issue with these provisions.

Clarify the authority of the Defence Imagery and Geospatial Organisation

I have no issue with these provisions.

Matters the Government is considering

Amend the ASIO Act to create an authorised intelligence operations scheme

I strongly object to these provisions.

ASIO has not yet made the case that the scheme is necessary, other than in strict hypothetical terms in the Discussion Paper. While it raises the possibility that an Australian agent could be prosecuted for receiving training from a terrorist organisation, that hasn't actually happened to date, and ASIO has not provided any examples of prosecutions which could not be secured, or investigations that could not be carried out, due to those limitations.

Creating a scheme by which the Director-General of Security can secretly authorise criminal acts is anathema in a society that purports to fall under the rule of law.

If the Government proceeds with these measures, any "safeguards" built into the scheme will be void, because the Director-General of Security would have the power to instruct his agents to simply ignore them.

Similarly, safeguards, checks and balances, and other protections built into other parts of Australian law would be lost. For example, what value is there in this Committee considering limitations on warrants for Telecommunications Interception issued to ASIO when ASIO's Director-General of Security can simply authorise those performing interceptions to do them without warrants? Why would we need Ministerial authorisation prior to the gathering of intelligence on Australian citizens, when the Director-General of Security has the power to allow agencies to bypass the Minister?

Our nation has enough history of law enforcement corruption and malfeasance to justify labeling as "delusional" anyone who thinks we won't have more of it. It is foolhardy to entrust ASIO with power that's as open to abuse as this proposal no matter how far beyond reproach the *current* Director-General of Security might be.

If the allegations from Mamdouh Habib have any credence, the ASIO of John Howard's days was sufficiently corrupt to have Australian agents in Egypt and Guantanamo Bay witnessing torture. Is it wise to grant this kind of power to that kind of organisation without first running through it from pillar to post to make sure that any vestige of corruption has been excised?

Modernise and streamline ASIO's warrant provisions

I object to Named Person Warrants. Applying for multiple ASIO Act warrants appears to me to be a safeguard for the public, one of the things we make law enforcement agencies do to ensure that they've made an unimpeachable case. I'm not in favour of watering-down warrant requirements to suit ASIO's "efficiency."

The Discussion Paper is vague about the nature of devices ASIO purports to be unable to use in concert with partner agencies. I am unable to support the proposal pertaining to Surveillance Devices until more information is offered.

I have no objection to Person Search warrants, provided they are for specific named persons or interest, and not for any person who happens to be at or near a searched premises.

I have no objection to authorisation lists for warrants, provided the persons on the authorisation lists would otherwise qualify as officers and employees able to execute warrants under the current version of Division 2 of Part III of the ASIO Act.

Clarify ASIO's ability to cooperate with the private sector

I have no objection to this proposal.

Amend the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act

I object to section 92 in its current form. There have been times in recent history when it would be in the public interest to identify ASIO officers, specifically those who are likely to be involved in criminal acts.

I would not support any strengthening of section 92 unless and until it is amended to include a workable public interest exception.

Matters on which the Government expressly seeks the views of the PJCIS

Modernise and streamline ASIO's warrant provisions

I absolutely do not support ASIO's use of third party computers and communications in transit. It is fundamental to our society that parties who are not the subject of an investigation ought not have to concern themselves with the police. One does not handwave past the "privacy implications" by alluding to unstated safeguards and accountability mechanisms.

Despite the casual and comfortable wording of this section of the discussion paper, what it is actually suggesting is breaking in to the computers of innocent third parties to inject what the third party would describe as a "virus" or "malware"; or hacking into stored, unread communications on their servers to add viruses or malware; where said viruses or malware contain surveillance software intended for the subject of a warrant.

As a law abiding citizen, I should not have to employ additional security measures to protect my computer infrastructure from my own Government just in case they happen to have a warrant naming someone to which I might send email. I should also not need to accommodate the risk of system failure, data loss or financial loss due to ASIO's insertion, deletion or alteration of data.

I absolutely do not support the Incidental Entry proposal. If ASIO wants to gain access to a premises, it should get a warrant. If it then becomes apparent they they need access to a different premises, they should get a different warrant. If they can't justify the second warrant, they shouldn't enter the premises. It's that simple.

I have no objection to the proposed amendments on the use of force provision.

I might support the Evidentiary Certifications proposal if ASIO had provided any examples of cases where they were unable to proceed due to its absence; But since they haven't, I object. Repeating from earlier: Their job is not supposed to be easy. Without evidence of actual harm, we aren't supposed to adjust our expectations and norms to make law enforcement and intelligence more efficient.

Amend the Intelligence Service Act 2001

A careful reading of the Ministerial Authorisations proposal depicted on page 11 of the Discussion Paper suggests that it seeks to amend the Intelligence Services Act to enable the Minister of an IS Act agency to authorise producing intelligence on an Australian person, where the Minister is satisfied that the person is, or is likely to be, involved in intelligence or counter-intelligence activities.

This needs to be considered carefully to account for the fact that "journalism" and "intelligence-gathering activities" are virtually indistinguishable, and it isn't the Australian Government's place to be investigating journalists.

As such, I do not support the proposed amendment, particularly given Australia's appalling track record in relation to Walkley Award winning journalist and Australian citizen Julian Assange.

I believe Mr. Assange carries out journalism focussing on the intelligence community. The Government plainly believes that he carries out intelligence-gathering activities, and has indicated through its Ambassador to the United States that it sees no impediment to him being extradited to face charges under the US Espionage Act.

While the Government continues to behave in that way, I am unable to support the Ministerial Authorisations proposal.

I have no objection to the ASIS cooperation on self-defence and weapons raining proposal.

Summary

In statistical terms, *almost nobody* in Australia will be investigated for a serious crime.

Yet much of this discussion paper proposes measures which would "simplify", "streamline", and "modernise" extensive electronic surveillance of almost everybody.

The nature of the relationship between citizens and the state is an important matter of political principle. We often make the mistake of believing we elect MPs solely to represent our interests; We also elect them to represent our ideals and principles.

During the last decade of National Security Legislation amendments, I don't feel that democratic principles have been honored. All too often I see lip service being paid to "safeguards", where checks and balances are considered acceptable to be written into legislation only if they're malleable enough that they can be bypassed.

The pendulum has swung too far, now it's about time it swings the other way for a while.

We're in an era where violent crime is at its lowest rate in Australia since the second world war. The worst example of terrorism in Australia which ASIO can muster is a collection of mentally disturbed wanna-be's prosecuted over four years ago. Australian organized crime seems like a big deal, but only if you leave your skepticism at the door.

We're a fundamentally safe country: Politically stable, prosperous, confident. The kind of place where a house break-in still makes the nightly news, *because break-ins are so rare that they're newsworthy.*

There is no better time than the present to start reassessing the nature of the relationship between the polity and the police.

Given that we are so safe and so crime-free, do we need to keep giving more and more surveillance powers to law enforcement and intelligence services?

Given that we know our security infrastructure is so relaxed and cheerful that anyone who really wants to produce mayhem probably can, we can interpret the lack of mayhem as evidence that nobody wants to create it. And if nobody wants to create mayhem, why do we keep funneling so many extra millions of dollars every year into our security services? What incremental value are we getting in exchange for those extra resources?

From my position as a regular citizen, it seems to me that very little of our National Security apparatus is controlled by rationality. It's mostly controlled by fear: We pay people in ASIO, ASIS, and other acronym-laden organizations to dream up awful scenarios and play, "What if?" games with them, and the end result is that we have a National Security policy that's dominated by whomever has the most pathologically overactive imagination.

The other issue that seems clear to me in so many diverse areas of policy is that the Australian Government harbours a deep distrust of the Australian people.

In a democracy it should work the other way around: The Government should trust voters to make good decisions about the kinds of people they elect to represent them, and voters should have every expectation that the Government will mess it up, and demand strong and effective checks and balances to make sure they don't.

In Australia the voters seem to be doing their job adequately, with levels of Government trust at near historic lows. But the Government is not doing its job: The Government is not trusting the electorate, and, at least in relation to our security services, it's not carrying out its duty by implementing adequate checks and balances to protect the electorate's interests.

How is it that we can have the AFP, ASIO, ASIS, and other agencies I'm probably not even authorized to know about, propose that I'm so mistrusted that I need to have the last two years of my communications logged in excruciating detail, just in case I one day commit a crime?

The Government needs to do better.

Stop being frightened of everything; replace fear with rational decision making, where we understand that we don't need to panic just because the Americans are panicking on "24."

And live up your side of the democratic social contract: You're supposed to live within strict constraints, unavoidable checks and balances, and have faith that we voters will generally get it right.

Lowering the standards on search warrants, creating offence provisions for not decrypting data, and implementing data retention systems aren't compatible with those principles. As a Government, you were wrong to ever propose them in the first place. Now please, withdraw them, and help us enjoy our historically safe society by letting the pendulum swing the other way for a while.