Submission to Parliamentary Joint Committee on Intelligence and Security on 'Equipping Australia against Emerging and Evolving Threats'

Chris Berg &
Simon Breheny

August 2012

Institute of Public Affairs
Free people, free society

Introduction

The Institute of Public Affairs believes many of the national security proposals contained in the Attorney-General's Department's *Equipping Australia against Emerging and Evolving Threats* Discussion Paper are unnecessary and excessive. Many of the proposals:

- Curb civil liberties;
- Systematically breach Australians' right to privacy, and;
- Breach basic rule of law principles.

The Discussion Paper offers at least 45 distinct proposals. This submission does not attempt to address each one. Instead, we focus on one particular proposal that the government is seeking views upon: the data retention policy that would require internet service providers to retain data on all users for up to two years.

The data retention proposal, along with a number of other proposals listed in the Discussion Paper, would be a significant increase in the power of security agencies and the Attorney-General's Department.

Are the proposals justified?

General principles of democratic governance demand that the more significant the extent of proposed new government powers, the higher the threshold for justification of such powers. Many of the powers proposed and raised in the discussion paper go significantly beyond the current security framework.

Significant new powers require significant justification. Yet the discussion paper makes only a very weak attempt at explaining the rationale for the proposals. The discussion paper makes reference to a general threat of cyber-terrorism, failing to adequately engage in the question of how these expansive powers are required to face real threats to Australia's national security.

The government has not demonstrated that the major security threats posed by terrorism are not sufficiently dealt with under existing security laws. In February 2010, the federal government's Counter Terrorism White Paper argued that "terrorists have not shown a strong interest in conducting cyber attacks."[1] Yet in June that year the Attorney-General's Department was already investigating the possibility of data retention.[2]

Justifications based on out-of-control cybercrime similarly need to be approached with a sceptical eye. Certainly, criminal activity is increasingly adopting an electronic dimension. But the committee must be careful taking too much of this at face value. Security agencies and commercial retailers of security equipment have massively inflated the economic costs and consequences of cybercrime in

[1] http://www.dpmc.gov.au/publications/counter_terrorism/docs/counter-terrorism_white_paper.pdf
[2] "Fury at Government proposal to retain web browsing data of all internet users", *PM*, Radio National, 11 June 2010

recent years.[3] The Discussion Paper does nothing to dispel such scepticism, and the committee should strive to determine a more concrete idea of the criminality risks that these new powers are intended to suppress.

Nor has there been a groundswell of community support for the government to increase their powers in relation to the supposed threat posed by cyber terrorism.

Between 2001 and 2011 there were 54 separate pieces of anti-terror legislation passed through the Commonwealth parliament.[4] This extraordinary legislative activity dramatically expanded the scope of law enforcement agency power. The Attorney-General's Department seems to believe that this decade of increased new powers itself justifies further increases: the paper stresses the need for "holistic reform" to telecommunications interception powers, in contrast to the scattershot changes over the last decade.

Given the current security environment the only remaining rationale is that the proposed powers will generally assist authorities in their enforcement role. This is not commensurate with the extraordinary nature of the powers proposed. The Discussion Paper does not offer evidence of an imminent cyber security threat which would require the extraordinary security powers proposed in the discussion paper.

Data retention

The most concerning proposal is the long-discussed data retention regime. The proposal, which would force all internet service providers (ISPs) to capture and store data on the activity of its users for up to two years is onerous and represents a significant incursion on the civil liberties of all Australians.

The IPA has been opposed to the federal government's data retention proposals since they were first publically mooted in 2010.[5] Data retention would be a continuous, rolling, systematic invasion of the privacy of every single Australian, only justified because a tiny percentage of those Australians may, in the future, be suspects in criminal matters. Indiscriminate data retention is an abrogation of our basic legal rights. Data retention regimes make internet users guilty until proven innocent.

We recognise that digital communications make it more challenging for law enforcement agencies to retrospectively track our activities. The government is eager to have similar capacities for dealing with digital communications like Skype calls as it has with telephone calls.

But mandatory data retention for digital is not analogous to keeping records of telephone calls. Phone companies collected their customer's data for billing purposes already; those existent records were available under warrant. By contrast, mandatory data retention policies would necessitate the creation of a massive *new* record of customer activity. As the privacy and online rights campaigner Geordie Guy has put it, "This is not a case of justifying access to information about your person that

[3] See Chris Berg, One hack of a crime wave, or so they say, Sunday Age, 26 June 2011; Peter Maass and Megha Rajagopalan,"Does Cybercrime Really Cost $1 Trillion?", ProPublica, 1 August 2012

[4] George Williams, 'A Decade of Australian Anti-Terror Laws' *Melbourne University Law Review*, v35 2011

[5] Chris Berg, "Taking Liberties", *ABC The Drum*, 15 June 2010

exists anyway, this is mandating the creation of personal information about you for the sole purposes of understanding your behaviour and affairs extra-judicially."[6]

The privacy consequences of such an enormous data creation program are profound. A decision in 2009 by the Romanian Constitutional Court overruling that country's data retention policy argued that no conception of privacy could be sustained if data retention existed:

> The regulation of a positive obligation that foresees the continuous limitation of the privacy right and the secrecy of correspondence makes the essence of the right disappear by removing the safeguards regarding its execution. The physical and legal persons, mass users of the public electronic communication services or networks, are permanent subjects to this intrusion into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communication, thus excluding the main communication means used nowadays.[7]

We agree. The imposition of such an extraordinary, systematic and universal program would render any presumed or existent Australian right to privacy empty.

There are also serious practical concerns with the proposals. The creation and long term storage of such a large amount of data would be highly risky. ISPs would be responsible for the security of that data. There have been a number of recent, high-profile data leaks from government and corporate organisations. Mandating the creation and storage of even more data would exponentially increase both the risk of these leaks and the potential damage from having done so.

The economic consequences of the data retention regime are also negative. Forcing internet service providers to capture and store user data for any period of time is a decision that will result in higher costs for internet service providers. New regulations would act as a further barrier to entry thereby further impacting competition between internet service providers, ultimately giving consumers less choice.

In 2010, the European Data Protection Supervisor Peter Hustinx said that "It is still highly doubtful whether the systematic retention of communication data on such a wide scale constitutes a strictly necessary measure."[8] This remains the case. Australian law enforcement agencies have a wide range of powers to access existent information on suspects without abrogating the privacy of every single Australian citizen.

Strictly limited, supervised, and transparent data preservation orders on targeted suspects would strike the right balance between individual rights and law enforcement. We note, however, that at this time no such correct balance has been struck. (For instance, the government's Cybercrime Legislation Amendment Bill would give all Commonwealth agencies – not only law enforcement agencies – the ability to issue data preservation orders.) The government should certainly not be granted new data preservation powers until legal protections on privacy are respected and law enforcement capabilities strictly delineated. The larger data retention proposal contained in the Discussion Paper should be rejected outright.

---

[6] Geordie Guy, "Why Data Retention is a Bad Thing", *GeordieGuy.com*, 12 July 2012

[7] Constitutional Court (Romania) Decision no 1258, 8 October 2009

[8] Peter Hustinx "The moment of truth for the Data Retention Directive" Brussels, 3 December 2010

Other civil liberties and rule of law problems with proposed new powers

There are a wide range of further proposals in the discussion paper which are excessive and disproportionate.

Many of the proposals contained in the discussion paper involve a high degree of ministerial discretion. The proposal to allow the Attorney-General to unilaterally vary a warrant is one such proposal. Courts are in the best position to issue and vary warrants and the processes in the warrant application process are appropriate. Powers of variation in the hands of ministers would be a rejection of the current court process, risk political manipulation, and would encourage secretive deals with law enforcement agencies.

The discussion paper also contains a proposal to amend the Intelligence Services Act to "add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities". The lack of definition around this new ground of ministerial authorisation allows for an extremely broad interpretation of the provision. Any number of activities involving the legitimate collection of information could fall foul of this provision.

The proposal to extend the default period of time that warrants are made out for is also concerning. Police and other security agencies should have only a small window in which to search a person or premises. The result of such a proposal is to have the threat of a search of one's person or property hanging over the head of anyone being investigated by security agencies for a longer period of time than is absolutely necessary. The test for search powers should not be 'what is in the best interest of the investigating agencies,' yet this is the test that appears to have been applied. Another clear breach of the rule of law is the proposal to give security agencies the power to remotely access computers and delete, move, and plant data.

State power should be strictly limited and those powers carefully delineated. Excessive ministerial discretion is incompatible with this conception of a legal system and creates a situation where it is impossible to comply with the law because the mind of the lawmaker cannot be known.

The data retention proposal should be rejected outright. The Institute of Public Affairs recommends that all other proposals in the Discussion Paper should be critically assessed under principles of proportionality to the potential threat, a proper assessment of what that threat constitutes, and guarantees of basic rule of law principles adopted.