Submission No 137

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Bruce Arnold

The Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600

Inquiry into potential reforms of national security legislation

I am writing in response to the call for public submissions regarding the Committee's inquiry into potential reforms of national security legislation.

Summary

Ongoing review and, where appropriate, enhancement of Australian national security and telecommunications law is desirable. Unfortunately the proposals from the Australian Attorney-General confuse bureaucratic convenience with necessity.

In considering the proposals the Committee has an opportunity to do two things. Firstly, it can explicitly reject the latest exercise in bureaucratic overreach, ie mandatory retention of telecommunication traffic data. Secondly, it can signal to government agencies and the Australian community that policy should have a substantive basis rather than being founded on ambit claims by particular agencies or a Minister's need to "be seen to be doing something".

It is axiomatic that a range of law enforcement bodies should have access to powers for action in the national interest. That does not mean they should have a blank cheque. The discussion paper accompanying the proposals does not substantiate claims that there is a need to change the existing surveillance regime and thereby impose substantial regulatory costs on business and erode privacy protection.

Background

The following paragraphs are informed by around thirty years experience in government, the private sector and academia regarding telecommunications regulation, national security, data protection and privacy.

I teach law at the University of Canberra. I am general editor of *Privacy Law Bulletin*, the leading privacy and data protection journal for legal practitioners. I have been active in advisory and policy-making committees of auDA (ie national internet domain name regulator), ISOC-AU (the Australian arm of the Internet Society) and IIA (the Internet Industry Association). My writing about privacy, computer offences, other areas of crime and telecommunications regulation has been cited in several hundred monographs, Australian and overseas official reports and peer-reviewed law and technology journal articles. I have also made invited submissions to a range of parliamentary committees and law reform bodies, with endorsement in their reports.

I have no consultancies or other commercial relationships that would reasonably be perceived as a conflict of interest. This submission is independent of the University of Canberra and does not necessarily represent the views of the UC Law School.

Data Retention

The retention by connectivity and hosting service providers (eg phone companies and ISPs) of telecommunication traffic information – and even of the content of that communication – have been a feature of proposals for at least 15 years.

Those proposals are predicated on one or more government agencies having direct access to that data for law enforcement or national intelligence purposes. They are also predicated on the data being maintained in formats that can be readily searched by the agencies. They reappear like the bogong moths that are a fact of life in Canberra: they're not smart, they're not useful, they're irritants that waste time.

Mandatory traffic data retention – whether it is for a period of two years or five years or ten years, depending on which proposal has been put to Parliament – has real costs.

It involves substantial costs for connectivity providers and content hosts in the public and private sectors (eg mobile phone service providers, webhosting services, libraries and universities) that are being asked to act as agents of the state. The network management systems used by those organisations typically feature billing and customer support facets. They are not concerned with long-term data storage, particularly storage in forms that can be readily parsed by government agencies. Restructuring those systems to provide storage is non-trivial. Its implications involve a reduction of competition in the ISP sector, driving small ISPs out of business, and imposing a tangible regulatory burden on entrants to the social network service market along with other entities whose clients engage in electronic communication.

Just as importantly, data retention has a cost in terms of privacy. That cost is real. It is an unacceptable cost in the absence of strengthened privacy protection[1] and more broadly in a justiciable right to privacy for all Australians that goes beyond the weak Commonwealth and state/territory privacy statutes. The cost has been highlighted in successive submissions by a range of legal and other bodies, with for example questions about phrasing such as "applying tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts".

Given demands on the Committee's time I will confine myself to quoting the submission by the Law Institute of Victoria, a body that cannot credibly be accused of radicalism or naivety about law enforcement.

In a previous submission about data retention the Institute commented that

> The large-scale collection of information by governments because it may be helpful to some government functions, rather than because it is necessary, constitutes a serious threat to online privacy. The power of the internet should not be used by governments to achieve measures of control that would not be possible without the internet. By way of illustration, the LIV suggests that neither

[1] Importantly, the discussion paper does not make links to the Government's proposals for updating of the *Privacy Act 1988* (Cth) and, as in the past, policy making about privacy, telecommunications regulation and surveillance appears to involve separate silos of officials with conflicting agendas and a reluctance to articulate common principles.

> government nor community would tolerate proposals to place telephone intercepts on all phone lines in Australia and record all conversations, or to open all mail, in case such information may be of use to law enforcement agencies. Such proposals would be unacceptable in a democratic society. There is no demonstrable reason why internet communications should be treated differently to other communications.[2]

Being able to open every letter, or have someone open the letters on your behalf (with or without a warrant), may well be convenient but is not necessary and is not desirable. Proposals for mandatory data protection should be condemned by the Committee, ideally condemned in a way that sends a clear message to policymakers who are obviously deaf to concerns that have been expressed over the past decade.

The *Sydney Morning Herald*, in reporting on the proposed changes, stated that Assistant Commissioner Neil Gaughan of the Australian Federal Police High Tech Crime Centre had commented

> "If we don't have a data retention regime in place we will not be able to commence an investigation in the first place. And it's already getting increasingly difficult," he said. Opposition to such laws in Germany - the government has declared them invasions of privacy and forbidden them - has left the German federal police agency the Bundeskriminalamt or BKA a laughing stock, Assistant Commissioner Gaughan said.

Changes to Australian law should be made on the basis of substantive need, rather than anxieties among Australia's police that people will laugh at them or hyperbole that law enforcement will be impossible without new powers.

Contrary to Assistant Commissioner Gaughan's reported claim, law enforcement has not ceased in Germany. It has not been prohibited or fundamentally inhibited by the German legislature or German courts. Germany's courts, along with that nation's businesses and society, *do* however expect German police and national security bodies to operate within the law and respect basic principles regarding privacy as a foundation of human dignity and a liberal democratic state. German jurisprudence over the past ten years has strongly emphasized that law enforcement personnel must follow the rules and that bureaucratic convenience does *not* trump fundamental rights.[3] We should have the same expectation in Australia.

The Committee should thus hesitate before endorsing a bureaucratic wish-list. Are the proposed changes truly needed? What are the costs? Do they serve to legitimate an ongoing process of regulatory creep – a drip by drip erosion of commercial freedom and civil liberties (first retention for two years, then for twenty, then for content rather than traffic?) without commensurate benefits for society and without meaningful supervision of ministers and officials?

---

[2] Law Institute of Victoria submission to Senate Committee inquiry into *The Adequacy of Protections for the Privacy of Australians Online* (nd), p2

[3] See for example the German Constitutional Court's 2010 decision on data retention - Federal Constitutional Court, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (Judgment of 2 March 2010), English text accessible as media release no. 11/2010 of 2 March 2010 at http://www.bverfg.de/pressemitteilungen/bvg10-011en.html

The Committee's response to the above comments might be 'what is the fuss … the Attorney-General has walked away from the data retention proposal'. Telecommunication sector businesses, legal practitioners, civil society advocates and ordinary Australians are concerned that

- the data retention proposal will not stay dead – it has been consistently criticised in a succession of reports but keeps on reappearing, with a disregard of strong criticisms expressed by business and bodies such as the Law Institute of Victoria
- the proposal appears to be driven by bureaucratic convenience rather than a substantive need.

The Committee has an opportunity to signal that Governments (and particular agencies) should address the criticisms and make a persuasive case rather than recurrently relying on rhetoric. In essence it is time to drive a stake through the monster's heart before it climbs out of the grave yet again.

The Attorney-General's discussion paper features impressive statistics about assaults and homicides on page 16. However, it is unclear what - if anything - telecommunications (or the Australian Security Intelligence Organisation) has to do with those deaths. The hard data is that most of the deaths involved kitchen knives, fists, frying pans, broken bottles and other implements. As far as I'm aware no-one in the past three years has been clubbed to death with a mobile phone. The nature of those crimes means that enhanced powers for the Australian Federal Police and ASIO (and mandatory data retention) would be irrelevant.

It is disappointing that the discussion paper is so disingenuous; the Committee might use the opportunity to call for meaningful information that supports the proposals and to strongly condemn the reliance on headlines rather than substance.

Law Enforcement Changes

The proposals are vague. It is thus difficult to determine whether they represent a true improvement or are instead 'one step forward, two steps backward'.

In dealing with the *Telecommunications (Interception and Access) Act 1979* (Cth) the discussion paper for example refers to "strengthening the safeguards and privacy protections under the lawful access to communications regime", with an examination of that Act's "privacy protection objective" alongside reducing the number of agencies eligible to access communications information and standardizing "warrant tests and thresholds". Those agencies range from the Australian Federal Police (and its state counterparts) to the Australian Competition & Consumer Commission and Centrelink.

However in "streamlining and reducing complexity in the lawful access to communications regime" the Government proposes to simplify "the information sharing provisions that allow agencies to cooperate". Restricting the number of agencies that can directly access communications information is desirable but is of problematical value if restrictions on the sharing of information are weakened. Establishment of a 'one-stop-shop' is attractive for the Australian Federal Police or

ASIO in competition with other bodies for funding but there is little improvement if those bodies simply act as agents for the likes of Centrelink.

Trust

Proposals for comprehensive data retention, for the sharing of information by a wide range of public sector bodies at the national and state/territory levels, and for substantially stronger interception powers by law enforcement and national security agencies raise concerns among the Australian community.

Many of those concerns are strongly held and often vigorously expressed but unfounded. They reflect

- ignorance about current legal frameworks, which provide law enforcement agencies with substantial powers
- a 'conspiracy theory' view of government, of Australian law enforcement agencies and of the global national intelligence community
- a disregard for the realities of drug trafficking, extortion, terrorism and other crimes.

However, some concerns **do** have a substantive basis. Disingenous policy documents and bureaucratic overreaching erode the trust that is fundamental for both law reform and the operation of agencies that by their very nature cannot disclose much information about their activities. We are asked to believe that ASIO, the AFP and other bodies are effective and respect the law. We cannot and should not know everything about what happens in those bodies. In turn, those bodies – and Governments – must show that they are worthy of our trust. Requests for additional power should not be automatically endorsed merely because there is reference to homicides, drugs, child sex offences or 'national security'. Bad policy – especially bad policy badly articulated – erodes trust, disrespects Parliament and fosters the misplaced anxieties that I have noted above.

The Committee can address those anxieties by highlighting 'national security' is taken seriously but is *not* a free ticket and that strengthened law enforcement powers should be closely tied to strengthened privacy protection. If there is a substantive case for stronger powers the Government should and can make that case in its dialogue with the Australian community rather than pointing to irrelevant statistics. Many legal practitioners and academics will strongly support policy that has a substantive basis and that situates law enforcement within a coherent legal framework.

Bruce Arnold
University of Canberra
19 August 2012