Submission No 123

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Alex Pollard

SUBMISSION TO INQUIRY INTO POTENTIAL REFORMS OF NATIONAL SECURITY LEGISLATION

Addressing the terms of reference

> 3) The Committee should have regard to whether the proposed responses:
>
> a) contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector

The War On Encryption

Changes under consideration include proposals to make it a crime to fail to assist with an attempt by a government agency to decrypt data (Proposal C. 15 a). Together with vaguely defined proposals for "record-keeping" and retention of communications data (Proposals A. 1. c., and C. 15. c.), a trend is emerging in public policy toward criminalising encrypted data and communications.

There is a parallel here with the failed "War on Drugs". The initial response by government is criminalisation, which though principled and well-intentioned, is impractical. With passage of time, the measures prove counter-productive or ineffective. Further measures are applied iteratively, criminalising victimless conduct, and wasting public resources on an unwinnable war. The principles underpinning the failed policies are never challenged – the solution is always more laws, more regulation, more taxpayer money, more police and more prisoners.

Similarly governments and law-makers may get it into their heads that the right and principled approach to the problems at hand are to retain communications and force people to assist in decrypting data.

This is putting us on a "slippery slope". Interception of communications by default requires the interception of all traffic, from which only relevant parts are retained. If communications in principle should be intercepted, what about encrypted communications, such as Transport Layer Security? How is secure web browsing (with https://) or secure email traffic to be examined? Do foreign and domestic website operators require a "license to operate" under which they must retain data on Australian users? Is there a sanction for failure to comply, such as blocking the site altogether? Are secure tunnels and Virtual Private Networks to be criminalised? Must ISPs perform a "man in the middle" attack on their customers' encrypted traffic – effectively banning encrypted communications? Or is the Australian Government better placed and more trusted to perform this attack on everyone?

The committee must consider very carefully whether it wishes to entrench a policy stance which will inevitably lead to a "War on Encryption".

Interfering With Computers

With regard to proposals to further enable security agencies to interfere with private computers in an otherwise illegal manner (Proposals B. 11. c. and C. 17), there needs to be greater clarity about the ability of agencies to plant incriminating data on a computer.

For instance, could an agency be permitted to plant incriminating information on a computer so that it could later be "discovered" and used as a pretext for temporarily detaining a target? Does the committee believe that "dirty tricks" or "Psychological Operations" to shape public opinion of a target should be explicitly prohibited? What obligations should there be for security agencies to disclose interference with evidence if a matter goes to court? Is the burden of proof meaningless if a government agency can conspire in absolute secrecy to interfere with evidence and then cover its tracks?

Conclusion

The Parliament must be very careful to not enable the expansion of secret unchecked power, either by the agencies themselves, or by launching another failed "war", entrenching a policy direction under which future parliaments then seek to "fix" an inadequate regime on the presumption that the underpinning policy is correct.

I strongly recommend the committee pay heed to Bernard Keane's "Hypothetical: news from a national security future"
http://www.crikey.com.au/2012/07/23/hypothetical-news-from-a-national-security-future/

Alex Pollard