Submission No 35

Inquiry into potential reforms of National Security Legislation

Name: Dr J G Dowty

Organisation: Private Capacity

From: James Dowty
Sent: Wednesday, 1 August 2012 4:38 PM
To: Committee, PJCIS (REPS)
Cc: James Dowty

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Sent via email to pjcis@aph.gov.au

1 August 2012

Dear Committee Secretary,

Submission to the Inquiry into Potential Reforms of National Security Legislation by the Parliamentary Joint Committee on Intelligence and Security

I am writing to express my opposition to the proposal to compel Australian carriage service providers (CSPs) to retain detailed personal data on their customers for a period of up to 2 years. This data retention proposal (DRP) has been widely reported in the Australian media but it is only mentioned in very vague terms in the inquiry's discussion paper, perhaps on page 28 and in part 15c of the terms of reference. I have been unable to find any official information on the DRP, such as a statement on the Attorney-General's website, so I have been forced to rely on media reports for information about it. This is regrettable. In an authentic democracy, the government would actively seek the views of the Australian people on the trade-off between our privacy and our security which is at the heart of the DRP.

I am one of the millions of Australians who will be directly affected by the DRP. I understand that, in theory, only authorized enforcement agencies with appropriate warrants will be granted access to the customer data that the CSPs will collect. If this were guaranteed to be the only use of the data then I would support the DRP. In practice, however, the highly personal and detailed data stored under the DRP will present a very attractive target for criminals and even some foreign governments. Some of our nation's most sensitive data will stored in the hands of a few hundred private companies where it will be vulnerable to physical and cyber attacks (such as last week's successful attack by the hacker group Anonymous on AAPT). It is therefore possible or even likely that, in addition to compromising our privacy, the DRP will actually weaken our security.

The retained data will also be vulnerable to misuse by future governments. Once the data retention begins, legislative change could immediately give an unscrupulous government access to the web viewing histories, emails and text messages of their political opponents and constituents. While the current government might be staunchly opposed to such misuses of the retained data, there is no guarantee that the government of 2050 will be as trustworthy. Of course, the data which is currently retained by CSPs is also open to misuse in this way, but the inappropriate use of two years' worth of data is likely to be far more damaging than the misuse of a few weeks' worth.

The discussion paper does not make a strong case for the DRP and it does not consider any alternatives with less impact on privacy. For example, it might be possible to meet the needs of security agencies by retaining data only on people who satisfy objective criteria which are known to be strongly associated with serious crime.

Lastly, I think the DRP will have a subtle and harmful effect on the psychology of all Australians. The vast majority of Australians are decent people and we do not need or want the spectre of the government hovering over our most intimate moments.

Yours sincerely,

Dr James G Dowty