Submission No 119

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Brendan O'Flaherty

Sent: Monday, 20 August 2012 4:36 PM
To: Committee, PJCIS (REPS)
Subject: Submissions on the proposed reform to the Telecommunications Act 1979

Dear Mr Secretary,

As you are aware, the The Parliamentary Joint Committee on Intelligence and Security (henceforth referred to as the Committee) is addressing reform proposals 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. In response to an invitation to make submissions on these reforms, I have devoted considerable time in composing this submission. I would appreciate it if my concerns were addressed without the use of a stock reply.

Provided the short time given to address these reforms by the public, which could be perceived as an attempt to avoid an open discourse considering their implications, I have only been able to address reforms to the Telecommunications (Interception and Access) Act 1979 in this submission. Regarding this, I am concerned about the following reforms:
1. "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" and
2. "establish an offense for failure to assist in the decryption of communications"
I am concerned about the first because data retention without cause implies guilt and retained data can be stolen by third parties. I am concerned about the second because the task of law enforcement should not be the responsibility of the telecommunications industry, although they may provide services to law enforcement for a fee if required.

The reasons provided to justify these reforms are that
1. "the Telecommunications Interception Act is out of date" and so as to
2. "[enable] individuals to live in a society free from threat to personal safety".
These reasons are not sufficient to justify the proposed reforms. They will be addressed individually.

1. "the Telecommunications Interception Act is out of date"
The Telecommunications Interception Act has been amended 45 times since 2001.
The so-called "legacy assumptions" of this Act are listed here and refuted to being out of date as follows:

1. Communications to be intercepted are easily identified.
Packet-sniffing applications can be used to determine the origin (IP address) of packets as well as to provide information on the application(s) and operating system used to send the packets.

2. A stream of traffic to be intercepted can be isolated from the rest of the communications passing over the network.
Multiple packets from one IP address can certainly be isolated. Even with DHCP addressing, the IP address of a user does not change in the middle of a communcation in the same way that a person's phone number does not change in the middle of a conversation.

3. Carriers and carriage service providers (telecommunications companies and internet service providers) control the traffic passing over their networks;
4. Carriers and carriage service providers are the only entities which control public telecommunications

networks.
It is unnecessary to control the traffic passing over a network to observe it.

5. Intercepted communications are easily interpreted or understood.
The difficulty in interpreting intercepted communications is only changed by offloading the task to industry.

6. There are reliable sources of associated communications data that link people with identifiers and identifiers to communications
The header information of communicated packets contain the IP address of the sender and receiver. The citizen associated with this IP address is held by the ISP. A warrant for this information can be made.

7. A 'one size' approach to industry obligations is appropriate.
Drawing a distinction between voice and data is not justification for these reforms.

Thus, it cannot be said that the Act is out of date, with the exception of Assumption 5. This relates specifically to the assistance to decrypt communications, which is cost-effective for law enforcement only as a result of forcing industry to complete this task. It is computationally intensive to decrypt communications, and additional infrastructure will most likely need to be purchased in order to do so. It is unreasonable to force the telecommunications industry to provide this service without compensation. Indeed the service of decrypting data can be provided efficiently if and only if there is competition between companies to provide such services. More generally, there should be a clear separation between the tasks of interception and interpretation of data, which should be performed by the telecommunications industry and law enforcement respectively.

2. "[enable] individuals to live in a society free from threat to personal safety"
As stated in the document "EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS" use of digital communications by law enforcement does indeed assist in the apprehension of criminals. This is distinct from the gathering of evidence on citizens prior to reasonable suspicion of guilt. Under our law, the burden of proof lies with the accuser. Reasonable conditions as to the guilt of a citizen can and should be met before surveillance on that citizen is allowed.

One threat to personal safety which was omitted in this document was the threat to the privacy of a citizen's confidential information. Forcing ISPs retain information on its customers prior to its need constitutes a threat, as it will be made available to theft by third parties. It also absolves the government of its responsibility to safeguard such information once it has made it available. Secure storage of data is a service which should also be provided at a fee.

I urge you and the Committee to consider that law enforcement should be adequately equipped to both decrypt, store and interpret communications and to gather evidence prior to requesting that the telecommunications industry retain information on citizens. In addition, that it is not reasonable to hold ISPs responsible for the safeguarding of retained data nor the decryption of that data without adequate compensation, although such services may be provided by industry for a fee.

It is important to keep our response to the threat of terrorism in Australia from devaluing the country we are trying to protect.

Yours sincerely,
Brendan O'Flaherty