Submission No 59

Inquiry into potential reforms of National Security Legislation

Name: Dr Andrew G Fry

Organisation: Private capacity

18th August 2012

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

I am making this brief submission to the Inquiry into Potential Reforms of National Security Legislation to help balance public civic concerns against the security concerns which I have no doubt will be put well and forcefully by those who have been charged with maintaining our security.

I value the civil nature of Australian society and the rule of law as much as any, but am concerned that our current balance of privacy versus security might be tipped to an unacceptable extreme because it is technically feasible to do so, not because it is desirable to do so.

I address the committee as a private individual, albeit one with significant experience and knowledge of the field. I have worked across many parts of the IT industry and in academic circles for 25 years, and I hold an earned Doctorate in Computer Science.

I would like to address the specific matter of intercepting and recording internet traffic, and the treatment of encrypted data, as raised in the committee's discussion paper. Other matters, such as standardising warrant tests, providing for single warrants, and streamlining the existing legislation, seem less troublesome.

Background

The proposals raised in the PJCIS discussion paper seem to disregard some important features of our current and future information technology environment.

- Access to networks is largely and increasingly through "casual" connections. It is now normal for a laptop, tablet, smart phone, and even desktop computers to make their network connections using "wi-fi". Such connections are made on-the-fly - not requiring any pre-existing formal relationship between network provider and user. In these instances, the network generally has no knowledge of who is using it - so we cannot easily associate a connection, or the data sent on that connection, with a particular person.
- Similarly, much network access is through internet cafés, coffee shops and restaurants, libraries, or through other shared services. In these situations, there is no clear relationship between connection owner, computer user, and ISP.
- Very powerful encryption technology is freely available and widely used. Sensitive and personal data - email, financial or commercial transactions, and personal data - is routinely protected using strong encryption such as HTTPS or PGP/GPG. It is not practical to break these types of encryption.

- Communications providers generally transfer "opaque" data. While many ISPs provide some email and web services, most people take advantage of third party providers (e.g. gmail, facebook, twitter). The data exchanged with such third parties is typically strongly encrypted and largely meaningless (opaque) when viewed by intermediaries such as the communications provider. Third party providers are very often based and/or located outside Australia.

Concerning the Proposal for Intercepting and Recording Internet Traffic

I note that legislation currently permits suitably authorised bodies to intercept communications, that this covers various media (telephone, mail, and digital transmissions), and that this is used to great effect in specific investigations.

This existing approach – a warrant is issued and intercepts are made according to the warrant – seems to function well. The balance of privacy and security that this provides is widely accepted in the community. Should it be necessary, it would be acceptable to most people if legislation were modified to clarify that the existing type of warrant-then-intercept action extends to digital communications.

However it has been widely discussed, and is proposed in the discussion paper, that it be mandatory for communications providers to retain summaries of all internet communications for two years. This raises several concerns:

- Should it be implemented, this proposal effectively renders all warrants retrospective, for a period of two years. Retrospective legislation and actions have been widely condemned across various fields, and are surely unacceptable in this case.
- If internet connections are to be logged, then internet communications would be substantially less privileged than the same communication made by traditional mail (“snail mail”), by telephone, or by courier. This will be unacceptable to most people who have sufficient technical knowledge to appreciate the situation. Such logging would have the obvious side effect of moving “interesting” communications back to traditional media, and outside the logged domain.
- Existing privacy legislation, and community mores, prohibit recording of private information except where a genuine need for the information exists. The proposal to record and store all connection/email details is contrary to those mores.
- The retention of large amounts of (potentially) very private, personal information raises to unacceptable levels the probability of frequent, major privacy breaches. Existing data holders (banks, hospitals, government departments, and ISPs) have widely blemished records of ensuring privacy, even when required under legislation – the level of leaks, hacks, and disruption could only get appalling when you consider the vast amounts of private information that it is proposed be retained for two years.

The proposal will be of limited use due to ease of circumvention, either by very strong encryption, obscuring message content, or by transmission using other media. Techniques for encryption and obscuring are widely known and systems easily available. Surely the limited benefits of large-scale logging are greatly outweighed by the costs to privacy and the conflict with community expectations.

The existing approach to communications intercepts (intercepts being permitted after specific warrants have been issued) has been effective and acceptable for many years. That approach can be extended to internet data without requiring record keeping, or retention of any historical data.

Concerning the Proposal for an Offence of Failure to Assist with Decrypting

When it comes to requiring assistance to decrypt data, the PJCIS discussion paper is somewhat vague concerning the parties and circumstances being considered. Three possible cases come to mind: requiring individuals to decrypt their own data on demand; requiring communications providers to grant access to data streams that the providers have encrypted to ensure privacy; and requiring all encryption to be easily broken.

Case 1. In the first case, any requirement that a computer user must decrypt their data, or to provide decryption keys, is in direct conflict with Australians' common law right to silence. The vast majority of Australians would find it completely unacceptable that this fundamental right be tossed aside.

Australian law drops our right to silence only in a few specific cases. Where decryption is demanded under one of those cases, existing law would apply, and no additional requirements are appropriate. Should decryption be demanded outside those few specific cases, it would raise everyday telecommunications intercepts to the status of a Royal Commission.

Case 2. In the second case, requiring a communications provider to decrypt their data stream, I merely note that it seems reasonable to require communications providers to assist, where a warrant applies, in decrypting the traffic which they are responsible for encrypting, such as a data stream encrypted for privacy by a Telstra endpoint (for example) and later unencrypted by the same provider.

Case 3. In general, the state of encryption systems is sufficiently advanced that it is easy for any computer user to encrypt information using commonly available tools or systems, such that decryption by a third party is completely impractical. In such situations, requiring (say) an encryption software provider, or network service provider, to break an encrypted message is technically ridiculous and would make a mockery of legislation.

Similarly, due to the global nature of computer systems, requiring locally available encryption systems to have some “back-door” (permitting easy decryption) would be largely pointless as strong systems are freely available globally. I note that the mere discussion of “back-doors” for certain encryption protocols was very strongly condemned in America, led to the development and use of alternative protocols, and was the trigger for wide-spread disregard for the official protocols rumoured to be tainted.

Concerning the Discussion of Strong Identifiers

There has been some community discussion of the implementation of “global” (or at least universal within Australia) ways to identify the communications or communications accounts of an individual (for example, requiring ISPs to record a passport or drivers' licence number).

The widespread availability of anonymous access points (casual network connections such as wi-fi or internet cafés) means that such identifiers are already of very limited utility.

Summary

While the logging and data retention that is proposed may assist in detecting or convicting some particularly stupid criminal activity, it will be of only limited value and is very strongly contrary to community standards and expectations.

The proposals for retaining records of IP communications are largely pointless, and contrary to community standards regarding privacy. These proposals should be dropped.

Any proposal that permits a demand for people to decrypt their own data will be contrary to common law rights and community norms. Such proposals should be dropped.

Any proposal concerning requiring a third-party to assist with decryption must be carefully considered, lest it be a pointless mockery.

Attempts to provide a common (global) identifier for communications users will be of very limited utility, completely impractical, and should be dropped.

Dr Andrew G Fry.