Submission No 71

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Ben Lever

Sent: Friday, 17 August 2012 5:22 PM
To: Committee, PJCIS (REPS)
Subject: NatSecInquiry Submission

To whom it may concern

Please find attached my submission to the National Security Inquiry

Regards

Ben Lever

Thank you for the opportunity to provide a submission to the inquiry. Firstly, I will discuss the broader issues, and then follow this with a point-by-point response.

The proposals that are most concerning are those of widespread data retention, and of forcing people to decrypt/give up passwords. While many other proposals are reasonable, prudent updates, and still others are impractical, inefficient or unintentionally bad, these two especially seem to be downright malicious.

Widespread data retention is the modern-day equivalent of steaming open everyone's letters, photocopying them, and leaving them in a warehouse - on the off-chance that a government agency might some day want to dig up the dirt on them. This is a mind-boggling invasion of privacy, it completely removes the presumption of innocence that a just democracy relies on, and can only be described as the formation of a police state.

Furthermore, it may be seen as "softening" them to not include ALL data, but merely metadata - that is, your IP address, the IP address of the computer you're talking to, perhaps protocols used, etc - but it is not. Metadata in aggregate is data - this is not the equivalent of just having a person's phone bill, but their library card and credit card records as well. And this is just from a home computer; if you have access to the metadata from a modern smartphone, you effectively have a tracking device in the owner's pocket at all time. We do so much through the internet, and constantly carry around a geolocated internet device, that even with just metadata you could construct a highly accurate picture of a person's day - which is of course the point. Such pervasive surveillance can only be justified on specific persons when warrants are issued - not on every single citizen.

In addition, there is little evidence that such a pervasive regime would even deter serious criminals, or result in more convictions. A German report[1], after a short stretch of similar data-retention there, concluded that there had been no improvement in serious crime statistics (neither a decrease in reported crimes, nor an increase in convictions) and that indeed there may have been a decrease in the capacity of law enforcement. It seems that under the current model - wherein most people are not surveilled, but certain persons suspected of crime are surveilled with warrants - many criminals will fail to take appropriate precautions, will use various telecommunication services, and will have that communication intercepted; however, under a data-retention model - wherein all communication between citizens is monitored - criminals know this and deliberately avoid using telecommunications, to the detriment of those listening in.

Therefore, while it may be appropriate to update surveillance capabilities to allow surveillance of more modern technologies, it absolutely must be done on a case-by-case basis with proper judicial oversight, and absolutely must not be done with blanket surveillance of all citizens, no matter how cheap or easy this might be for law enforcement agencies. This is especially true given that most branches of Australian law enforcement have at some point been massively corrupt, requiring Royal Commissions to fix; given that other countries with similar surveillance, such as the UK, have made huge mistakes by surveilling and arresting completely innocent people; given that Australian government agencies such as the ATO and Centrelink have repeatedly been embroiled in scandals wherein their employees accessed private

data inappropriately; given the unjustifiably heavy-handed response to environmentalist, labour, and Occupy movements by police forces from Melbourne to California. The law enforcement agencies that are asking for these changes have not exactly earned the benefit of the doubt - thus, the potential for abuse must be considered just as thoroughly as the best-case scenario.

Forced decryption too removes the presumption of innocence, but for different reasons. It is technologically possible to encrypt data such that it appears to be an innocent file - hiding text within a .jpg, for example. In a world where it is illegal to fail to decrypt data when ASIO asks you to, it is only logical that genuine criminals would encrypt their data in this way, rather than in an obvious way. This would effectively make the legislation useless on the one hand, or unbelievably totalitarian on the other. If ASIO cannot identify which files are actually encrypted and which are actually innocent, could they still throw a person in jail for failing to decrypt it? Not only does this remove the presumption of innocence, it violates the principle of corpus delicti - it would be impossible to even demonstrate that a crime (failing to decrypt) had even been committed.

The argument is made in Chapter 3 of the Discussion Paper that Australians have a reasonable expectation of privacy, and that these laws are being suggested as a means to that end. However, this is so antithetical to that cause as to be a complete farce - not only does it completely eliminate any expectation of privacy from the government, it presents a massive target to identity thieves and others who may wish to steal the data of Australian citizens. Creating a database that contained such comprehensive data on the online activities of Australian citizens creates an enormous privacy risk; in the extremely likely that at least part of this database were compromised, it would be an unmitigated disaster for the privacy of Australian citizens. It has been repeatedly demonstrated that corporations are not infallible when it comes to protecting their customers' data from hackers - AAPT's recent breach demonstrates this most appropriately. Further, the Wikileaks scandal, as well as a recent incident in which ADF personnel files were accidentally released, shows that governments cannot be trusted with this data either - not to mention that, for example, Victoria Police was involved in a scandal relatively recently whereby they had failed to properly destroy sensitive data (pertaining mostly to fingerprints) within the allotted timeframe.

As a final note, the definition of "serious crime" for the purposes of surveillance has been set at a seven-year jail term; this law has been stretched to include lesser terms, so that child exploitation could be included. This seems prudent as an interim measure, but is far from ideal - quite aside from it setting a precedent of allowing less serious crimes to attract surveillance until ANY crime is sufficient for all-out surveillance, it disturbs me greatly that child exploitation carries a sentence that short. The approach should be to increase sentences for small-s "serious" offences so they are within the scope of the big-S "Serious Offences" definition, not the other way around; though I understand this is beyond the scope of this submission.

Below follows shorter, point-by-point responses.

1. Strengthening the privacy safeguards is definitely a positive and necessary step in updating the TIA Act for the modern age. I am however slightly concerned at the wording of "examining" mandatory record-keeping standards,

given that it is kept quite vague and that later in the discussion paper there seems to be support for dramatically lessening record-keeping standards. Therefore, while I support this proposal generally, it is with the caveat that record-keeping standards must be maintained.

2. The number of agencies able to access data has indeed become bloated over the past few years, so I support the proposal of reducing the number of agencies who have access to only those who absolutely must have it. I also theoretically support the standardisation of warrants; however this support presupposes that they are brought to a reasonable standard, and that this is not used as an excuse to dramatically lower some thresholds under the guise of streamlining.
3. While there is potentially great benefit in simplifying the information-sharing process, there is also great potential for abuse. If this were implemented, the government would need to demonstrate that proper oversight would be in place - something it has not done here.
4. The answer to this proposal depends entirely on what happens with other proposals. If only a "targeted wiretap" approach to intercepting internet communications were implemented, some level of cost-sharing with ISPs and other such industry stakeholders might be appropriate - although, generally speaking, it is only appropriate for them to be made to provide the capability for intelligence agencies to do what they must; it would be inappropriate for ISPs to share the cost of the actual surveillance. However, in the scenario of a blanket data-retention program, like the one that has been suggested, sharing these costs in any significant way with ISPs would be incredibly burdensome, would put Australians at a competitive disadvantage in all areas requiring the use of those ISPs (which going forward will be *every* industry) and will be a major deterrent for IT companies considering doing business in Australia. Further, while the proposal suggests ACMA's regulatory role be clarified, the discussion paper does not clarify precisely what it means by this - it does not make clear what ACMA's role currently is, nor what it is envisioned to be.
5. I am perhaps not sufficiently aware of the legal machinations of warrants to comment too incisively, however the use of the word "varied" makes me hesitant. If the Attorney-General would only be allowed to vary the dates - that is, effectively renew the warrant without re-starting the legal process - then this would be fine, although some sort of limit on how many times this can happen would be necessary to prevent a single warrant being used to justify indefinite surveillance. If other details were able to be varied, however, this carries an enormous risk of abuse, as the effects of the warrant intended by the judge who granted it could be completely misaligned with its actual effects if enough variables were changed. Modernising the definition of "computer" is however a reasonable and prudent change.
6. These basic bureaucratic changes seem fine.
7. This proposal depends entirely on which bodies would be assisted, the nature of the assistance and the circumstances in which it occurred. As no such detail has been provided I must oppose this proposal, as there is significant potential for abuse that has not been accounted for.
8. As long as there is sufficient oversight in place, creating one warrant that can do a (specified, finite, case-specific) number of things seems like a reasonable streamlining measure.

9. This is worded so vaguely that it is difficult to tell precisely what is being proposed. However, my answer to Proposal 4 can be applied here - though I have dealt with the privacy implications above, the burden to industry would be significant under any large-scale surveillance regime, though I accept there may be some scope for regulating industry to ensure targeted, warranted surveillance is possible.
10. The discussion paper is not sufficiently clear, but I understand the proposal is essentially as follows: if it is anticipated as being necessary for an ASIO officer to commit a specific offence to maintain their cover with criminals they are investigating, a judge or someone else in an oversight position will exempt them from liability for this specific crime on this specific occasion. They will be provided exemptions only under specific circumstances in which it is necessary; they will be provided with exemptions only for specific offenses it is anticipated they must commit, such as receiving training from a terrorist organisation, and not given carte blanche for all potential offences; and they will not be allowed to commit these crimes indefinitely, being limited only to the time frame indicated. If this is an accurate summation of the proposal - and the violent/sexual crimes mentioned are not able to be pardoned, as mentioned - then this seems a reasonable proposal. However, I stress the need for careful oversight of this program, as it obviously carries enormous potential for abuse. Ideally, more than one level of independent oversight should be mandated.
11. This proposal has very distinct parts that must each be taken individually. Creating a named warrant, to specify a person under surveillance rather than a device, is a prudent update given the nature of communications technology ownership in the 21st century. Allowing this person to be searched independent of the premises falls within a sensible scope for such warrants, and clarifying who is able to execute these warrants (and training them accordingly) is necessary when changing the scope of warrants like this. However, allowing the disruption of a target computer necessitates a level of remote access that entails too significant a privacy burden, and I therefore vehemently oppose this portion of the proposal.
12. Again, clarity is sought in the laws, without any clarity being provided within the discussion paper. I cannot know what such cooperation with the private sector would entail and therefore I cannot support this proposal - although from what it suggests, I am inclined to oppose it.
13. This seems a reasonable proposal.
14. I vehemently oppose this proposal, on the grounds mentioned above
15. Establishing an offence for failure to assist in decryption is not only a massive invasion of privacy, but is also completely impractical. What happens if a person genuinely loses their passwords or encryption keys? Moreover, in the event that such a law did come into effect, it follows that anyone hiding genuinely illicit data of the type this law is intended to catch, would do so by encrypting the data into a form that looks innocuous - that is, making it appear to be another file. At such a time as this becomes commonplace among genuine criminals, what happens to the innocent person whom ASIO instructs to decrypt their holiday photos? One cannot make it illegal to fail to assist in an impossible task - and there would be no way of differentiating between uncooperative criminals and genuinely innocent persons. As to the data

retention proposal, I vociferously oppose this proposal on the grounds mentioned above.

16. I probably don't know enough about the mechanics of this proposal to comment, however some of the things I've read from better-informed people make me very wary - particularly with regards to the possibility that documenting the system architecture so extensively could in fact make it easier for malicious hackers.
17. The provision to allow third-party computers to be used to access target computers has enormous potential for abuse and is therefore unjustified. Unless some actual evidence is provided to show that such provisions are actually necessary - rather than just "Take our word for it that it's necessary" - nothing with this level of intrusion, potential for abuse, and potential for collateral damage, can be enshrined in law. The same applies to allowing access to third-party premises.
18. As I read this, it seems that what is suggested, is for certain activities that do not currently require warrants, to be authorised by the Minister. This raises the question for how exactly such operations are authorised now, and indeed what those operations might be - the paper is incredibly (and it seems deliberately) vague. Without concrete details on exactly what the Minister would be able to sign off on, and what would require a warrant, I am unconvinced that sufficient judicial oversight would be provided and therefore cannot support this proposal, at least until such time as clarification is provided.

This concludes my submission. Thank you for reading it.

Ben Lever

1. http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf