Submission No 126

Inquiry into potential reforms of National Security Legislation

Organisation: Arved von Brasch

Submission to the

Joint Parliamentary Committee
on
Intelligence and Security

for the

Inquiry into potential reforms of
National Security Legislation

by Arved von Brasch

1 Introduction

National security is certainly important. That is not in dispute. It is also the case that modern technology has significantly lowered the barrier of entry for all kinds of human endeavours, including organised crime and violence. National security can only operate well, however, in an environment of public trust. Public trust is currently under threat and contempt for law and government will increase unless strong safe guards are maintained monitoring intelligence agencies.

This is also the first age of big data[1]. Large datasets now exist which can be mined for all kinds of information. This is the first time such large datasets have been available and the processing power to draw conclusions from them has been available. While this clearly has some great benefits, such as predicting disease outbreaks, it has also led to unprecedented opportunities to attack privacy and other civil liberties. This creates a perception that government and a powerful elite have rights and privileges that ordinary citizens lack.

Certainly a violent death at the hands of fanatics, or even severe financial distress caused by espionage are not desirable outcomes. However, these risks must be understood in real context, and weighed against very real invasions of citizen's privacy and right to live their lives as they see fit. The right not to feel watched is also important.

1.1 National Security

The thwarted planned terrorist attacks trumpeted in the discussion paper were all avoided without the proposed changes. Clearly the current powers intelligence agencies have are sufficient, and perhaps already be too extravagant. Granted that this is very hard to quantify how effective money spent on intelligence agencies is. Our intelligence agencies certainly provide a valuable service, but because of their privileged abilities and covert nature, they must not be allowed to expand beyond parliament's or the judiciary's ability to provide proper oversight.

This is always a complicated issue. While there is certainly a risk that some people may be killed or otherwise harmed by malicious external forces, the actual risk is quite small. Albeit, the perceived risk is very large. Governments and citizens alike are prepared to risk lives for convenience in daily living. Fatal road accidents in Australia far exceed death and damage caused by terrorism. Unintended consequences should also be factored in. How many people choose to drive rather than fly because of the increasing inconvenience that air travel has? How does that contribute to road safety?

Security and safety is more than just having a low probability for the average citizen being killed or maimed by threats foreign or domestic. It is also about the perceived sense of safety and security. Indeed, this is the thinking behind much security theatre that is currently engaged in. On a straight up cost-benefit analysis, including opportunity and time costs, it provides very little if anything, but it does engender a feeling of 'something being done' in the average citizenry. The point is that humans are terrible

[1] http://radar.oreilly.com/2012/08/big-data-is-our-generations-civil-rights-issue-and-we-dont html

at estimating risk. More people are killed by cows than sharks, but there isn't a fear of cows in the population. While there is a strong, although probably declining, fear of terrorism in the community, it isn't clear that this fear is entirely justified based on actual risk. The question is how much should be spent on pandering to low risk - high fear scenarios when some of the resources spent here could dramatically improve the lives of many Australians in real terms.

At the end of the day it is hard to put numbers on any of this. There is really no way to calculate that X million dollars spent on national security reduces risk of terrorist attack by $Y\%$. That doesn't mean that no money should be spent on national security, but further emphasises that strong oversight is necessary to ensure the money is being well spent. Additionally, citizens are largely in the dark about the way intelligence organisations operate and how taxpayer money is used in this arena. This further makes it hard to grasp how well they are operating. This isn't helped when the reported costs of online criminal activities are repeatedly shown to be overblown[2].

1.1.1 Psychology

As a minor aside, there is an obvious perceived problem with the way people come to be employed by intelligence agencies. Now that psychological screening is a requirement, the kinds of personalities that are selected does present some concerns. While it is completely understandable that intelligence agencies do not want to employ people who are likely to leak sensitive information, this could create a workplace culture that is unable to adequately object to ethically questionable orders. Whistleblowers, while often unliked, are useful, even necessary to prevent organisations becoming toxic. Deliberately removing anyone likely to voice concerns with ethically questionable practices further emphasises that strong external oversight is required.

1.2 Australian Society

Australia is a fantastic place to live. Part of why it is so is that has strong roots in the philosophy of individualism. At least in the sense that every Australian is allowed, even encouraged, to pursue their own interests and forge their own lives as long as they do not bring harm, intentionally or otherwise, to others in doing so. In particular, they should be able to engage in normal activities without feeling that they are being watched or monitored. This requires fairly broad civil liberties. We should guard against risking what makes Australia great for perceived safety. That is essentially Benjamin Franklin's idea, 'They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety'.

What is important here is that as technology progresses, this is certainly going to become an arms race. That guarantees that any liberties surrendered will only be for temporary safety as those who wish us harm will simply develop new methods of achieving their goals.

[2] https://www.propublica.org/article/does-cybercrime-really-cost-1-trillion

1.2.1 Privacy

Privacy is still crucially important. The internet has given many minorities a voice that they otherwise did not have access to. While sometimes this allows minorities with malicious intent to congregate and meet in ways that were not previously possible, it has also allowed minorities that are otherwise unseen and ignored in society to speak for the first time. Such people require strong privacy so they are not killed. More generally, there are situations where many ordinary people require privacy to avoid harassment and unpleasantness for simply speaking unpopular ideas.

Online, privacy generally means two things, anonymity and encryption. Anonymity allows people with minority views or circumstances to express them without danger to their own lives. The cost is that it also provides cover to those whose minority views or circumstances are clearly at odds with society's wellbeing. Encryption is obviously necessary for trust. Online transactions cannot occur without it, and even in a home environment there is plenty situations where encryption can be employed for legitimate reasons. This is especially the case where most of the privately held computers with an Internet connection cannot be considered secure.

2 Response

First, lack of response to any particular proposal should not be deemed as an acceptance of it. Unfortunately, like many proposals of this type, little time was provided for public consultation. Ultimately, this discussion will have a far greater impact on the kind of country Australia is in the long term than the asylum seeker debate, yet it gets far less public discussion. Fortunately, this discussion paper appears to be reasonably balanced.

2.1 Telecommunications (Interception and Access) Act 1979

2.1.1 Establish an offence for failure to assist in the decryption of communications

This seems incredibly dangerous, depending on how 'assist' and 'failure' are defined.

There are numerous circumstances where a person may not be capable of decrypting stored communications. An obvious real example is the Wikileaks insurance file. The entirety of the cables were encrypted and public released. Without the password, this file was useless to the people who downloaded them, but it meant that many people would have access to the entirety of the cables in the event that Wikileaks was attacked and released the password. Regardless of the opinion of Wikileaks, or the outcome of this particular case, this is an example of a situation where many people may hold encrypted communication but be completely unable to decrypt it. It would be dangerous for this situation to become criminalised.

Additionally, there is also a flavour here of requiring people to incriminate themselves. While this is not a protection Australians have, it is generally frowned upon

when people are forced to generate evidence against themselves.

This is not a proposal that should be followed lightly.

2.1.2 Tailored data retention periods for up to 2 years for parts of a data set

Attempting data retention without a warrant seems like a fundamental invasion of privacy, and a major security risk. This data set would have incredible potential value to the dangerous element that this inquiry is concerned about. For major ISPs, it would be stored in a single place and would be vulnerable to being accessed. Such stored information would, necessarily, leak. The only way to avoid that is to not collect the information in the first place.

How would the private companies retaining such information be prevented from monetizing these records? Additionally, for an organisation the size of Telstra, the costs associated with implementing this proposal seem to be prohibitive.

This is not a proposal that should be allowed to go ahead under any circumstances.

2.2 Australian Security Intelligence Organisation Act 1979

2.2.1 Enabling warrants to be varied by the AG

The extension of the duration of search warrants from 90 days to 6 months seems dangerous. At the very least a monthly judicial review must be required.

2.2.2 Amending the ASIO Act to create an authorised intelligence operations scheme.

This also seems dangerous as a blanket change. The reasons to allow protection from criminal and civil liability are certainly valid. Perhaps if this operated as a valid defence from prosecution, with the requirement to explain how the actions were necessary for that particular operation.

2.2.3 Using third party computers and communications in transit

At the very least, the owners of the third party computers should be informed of the operation, in case they waste resources investigating what looks like a security breach.