Submission No 75

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Russell Stuart

Sent: Saturday, 18 August 2012 1:37 AM
To: Committee, PJCIS (REPS)
Subject: RE: Inquiry into potential reforms of National Security Legislation

I am a software engineer, and have been for some 30 years. I read your terms of reference with a heavy heart. There was a time I my life when I could reasonably expect that what I did in my private life remained private. But having been subjected to Moore's law for 30 years, I am keenly aware of implications it will have on the private life I have life. It will all but disappear.

Right now the people bearing the experiencing the sharp edge of this wave of change are our children. Fearing adverse publicity, intercepting their students posts on Face book and the web is now considered best practice in our schools. This includes looking at their encrypted connections, meaning those encrypted with the "https" protocol. As it happens it is relatively easy to perform what is called a "Man in the Middle attack" on https connections if you control the machine the student is using, which schools do. And so every email home, every tweet, every nervous teenage love letter, the first google of sex is recorded in case sometime later a student bullies someone, or threatens a teacher.

This inquiry is in being asked to comment on the merits of extending to this level of surveillance to every adult Australian. I think the merits will eventually make it be impossible to resist. The promise by law enforcement agencies of being able to prevent another Port Author massacre in exchange for giving a little privacy seems fair.

With this in mind I have two points to put to the inquiry. The first is on transparency. The march of Moore's law means the state, with the aid of it's computers, will be able to see into every Australian's life in a way none of us have experienced before. This is unavoidable, and to the extent it makes us all abide by the rules it is a positive change. But it also requires the shift of the knowledge of many when it is abused by people in a position to do so it becomes negative, as illustrated by the selective release of information in the Muhamed Haneef case. The Australian public needs to know what information is used, and when, and why. There is no reason why Australian's can't know what information their police force sought about them after the case is concluded, but to my knowledge this is rarely released. No one knows whose phone was tapped, how many email's were intercepted, the SMS's that were collected, or on what pretext.

The effort involved in collecting this data is no doubt offered as excuse for not collecting it. But Moore's law cuts both ways, so in an era where every request is handled by a computer this excuse isn't unsustainable. The effort involved is far less that what is proposed the ISP's do here, such as recording every email sent or received by every Australian. The real reason for not wanting to release the information is probably more to do with the push back they might get from the citizens who are worried about their privacy, but surely such push back is part of a well oiled democracy. In the end it is the voters who should be making the decision on how safe they want to be, and what sacrifices they want make to achieve it. They can only make that decision when they can see what is being record, and what it achieved.

The second point I want to make is in regards to demanding the release of passwords. Be aware the trade off for making such a demand is the possible punishment of an innocent person. This is because encrypted data is indistinguishable from random data, as illustrated by this quote from http://crypto.stackexchange.com/questions/1646 (AES stands for Advanced Encryption Standard, blessed as such by NSA):

> AES-CTR is supposed to be indistinguishable from random noise: if AES-CTR was distinguishable, then this would imply that AES (the block cipher) is not indistinguishable from a random permutation, and that would be viewed as a structural weakness in AES. ... No such structural weakness is known yet for AES

Like events that make no sense, there is natural tendency to call data you can't understand random. Or, if it suits your purpose, encrypted. Unfortunately other data can also look random, such as highly compressed data. See http://arxiv.org/abs/1001.3485 There are computer protocols (such as OTR, http://en.wikipedia.org/wiki/Off-the-Record_Messaging) that provide what is know as "Perfect Forward Secrecy". If a message encrypted with Perfect Forward Secrecy is saved it can't be decrypted even if you do know the password.

In short, a law that requires a person who is presumed innocent to reveal something he may not know is fraught with danger. I gather we already have such a law:
  http://en.wikipedia.org/wiki/Key_disclosure_law#Australia
I hope this inquiry will recommend adding defences to this law, defences that insist on strong evidence of the password being in the persons possession, and having been used recently.

Finally, this enquiry should consider the future implications of whatever they recommend. As I said, I've witnessed 30 years of Moore's law. It at least another 10 years to go, and if they manufacturers master 3D chips it may well be 10 decades. In a little while car registration number plate will become common place, so the government will potentially know where everyone drives, all the time. Mobile phone operators (and Google) know where you are, all the time. Queensland police have used go-cards (the travel card in Brisbane) to track witnesses of a crime. Credit cards track your every purchase. In 10 years it is likely face recognition will become very accurate, so those council camera's in public places will be able to track who is in the public rally.