Submission No 212

Inquiry into potential reforms of National Security Legislation

Name: P Potter

Organisation: Private capacity

To the Joint Parliamentary Committee on Intelligence

I write to object to the request by Australian law enforcement and security services to record all phone and internet activity for two years. I hope that the committee will consider my submission, even though it is late.

I've not done anything like this, writing to the Government, but I feel the need to raise my concerns over the limited amount of information provided by the media. Actually it's more like pleading.

Let me begin by asking the committee, do you lock the stall door when you go to the toilet?

Perhaps this is a crass example, but it highlights the proposal before you. After all, there is nothing secret going on, let alone illegal. Is it private, have I a right to this privacy?

Would you mind if there were cameras over each bathroom stall, just in case you were doing something bad?

We, all of us, have something to hide (if not everything). Privacy and secrecy are an inescapable part of the human condition. This may be a little too philosophical for the committee to care about, so I've tried to provide some more practical concerns.

Exactly who would hold all this information?

No matter was legislative measures you may put in place to guarantee privacy, the very first thing you would have to do is grant exemptions to companies on technical grounds in order to install such technology, and to check that the technology is working and information is being recorded. The Privacy Act has examples of such exemptions. This has the net effect of allowing staff at those organisations to access anything they want, whenever they like, on the flimsiest of technical pretexts.

There is also a problem of protecting such systems. You know full well that such systems will be breached. You've doubtless had countless IT and technology experts tell you over the years that it is a matter of 'when' security breaches occur, not 'if'.

The accuracy of information gathered would also be highly suspect. Voice recognition is very inaccurate, despite years of the best minds working on it. Internet connections are often shared amongst many people, as are phones and such. It would be too easy to mistake one person for another on such systems (let alone evidence tampering). I imagine that even I could easily have such evidence tossed from a courtroom.

Guilty until proven innocent?

In effect, you would be authorising the telecommunications interception of 22 million innocent people. To me, this sounds a lot like 'Everyone is guilty of something, we just need to find out what they're guilty of.' Where will this leave lawyer-client privilege? Whistle-blowers? Reporter-source confidentiality? The rights of a child? All of these important and lawful protections would effectively be removed.

Such information probably couldn't be used in a court of law, but it could (and would) be used.

The Australian police forces and intelligence services already have all the tools and technology they need to gather information on people they suspect of a crime or nefarious activity. I'm highly suspicious when they say that this isn't enough.

I would have like to have asked the assembled Police Commissioners before you, "What crimes would this prevent?" Of course, the answer is none. Not one.

What it will do is give law enforcement 'leverage' over people. "Tell us what we want to know, or would you like your husband to hear about these conversations with your ex-fiancé." "Give us what we want, or we'll tell your parents you're gay." Before you balk at that, put it to the Police Commissioners. Ask them if they've ever used someone's personal (and legally irrelevant) information against them.

You already know I'm right, so where exactly does the committee think this would end?

If you've nothing to hide, you've nothing to fear.

Growing up through the end of the cold war era, I learned about this one in primary school. It is the catch cry of the oppressor. Always has been, always will be.

If people aren't breaking the law there's no harm, right? Where would gay rights be if, in the 1970's, this technology was at the disposal law enforcement?

I ask you to give that some thought for a moment.

If you were gay, you were guilty of a crime. If you knew a person was gay and didn't report it, you were guilty of another crime. If you were even to admit to an urge or curiosity, without ever acting on it, you were under suspicion for life. And if you had any objections, authorities could 'accidently' release the fact that you were gay into the public domain.

There would have been lots and lots of people in prison. What's worse, the evolution of our society would have been completely suppressed and stopped. Dare I ask what would have happened to the union movement?

People are as they are, and do as they do. The law had to catch up to the people. I fear that you would see an end to this necessary (and messy) part of democracy.

What about the future?

Even if I could accept that your committee, law enforcement and intelligence services all have the purest of motives, you cannot be blind to the likelihood of abuse.

How easy would it be to ensure the peoples vote when you can simply blackmail them all? How simple would it be to ensure obedience by threatening to expose ones secrets? Why worry about protest when you can guarantee silence?

Your committee can offer no real protection against such things. In the future, who is going to complain when they're lives can so easily be destroyed?

It probably won't work.

Currently, I can bind my internet connection to an overseas VPN (Virtual Private Network) provider, far beyond Australian law enforcement, I can even add multiple layers of such. It is legal to do so, the ATO (for example) provide such a system for accountants to make lodgements, on-line banking couldn't work without it, etc. By doing so, I can encrypt all of my internet traffic so heavily that it would take all of the Governments computers years to break even the simplest of messages. I can use similar encryption on any and all voice conversations, or simply use a context based code.

I admit that I would consider doing these things to prevent you from monitoring me. Not because I have anything in particular to hide, but because I lock the toilet door too.

Who am I, to ask such questions?

I'm no one. I'm a nerd, one who is concerned that the Joint Committee on Intelligence is going to give away one of the principal and basic freedoms I was raised to believe in, the right to privacy. While I certainly understand the needs of law enforcement, this goes way too far.

I'm not as smart, eloquent or educated as all of you, but I hope that you recognise the danger of what you're considering. It has to outweigh the Governments need to enforce the law.

On my knees, I beg the committee. Please, reject this proposal outright.

Patrick Potter, South Australia.

"With the first link, a chain is forged. The first speech censored, the first thought forbidden, the first freedom denied, chains us all irrevocably." - source forgotten.