Submission to the Senate Legal and Constitutional Affairs Legislation Committee Inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013

Pirate Party Australia

Simon Frew (simon.frew@pirateparty.org.au)

31 July 2013

Pirate Party Australia supports the aims of the Telecommunications Amendment (Get a Warrant) Bill 2013.

The current system allows a high degree of warrantless surveillance. The *Telecommunications (Interception and Access) Act 1979* Annual Report for the year ending 30 June 2012[1] lists the number of requests for telecommunications data which require no warrant as the staggering amount of 293,501.[2] This equates to approximately one in 75 people having their metadata accessed without a warrant by intelligence or law enforcement agencies. This is a massive invasion of privacy of Australian citizens which needs to be reigned in and put under competent legal supervision. The question *quis custodiet ipsos custodes* — 'who watches the watchmen' — is particularly important given the vast amount of information that can be accessed. Invasive, widespread surveillance of literally hundreds of thousands of people does have a negative impact on society, that, unlike the much-touted benefits of surveillance, has been researched and documented. While the German data retention regime was in effect, the research institute Forsa surveyed Germans and found that one in two people refrained from conducting personal medical research online due to privacy concerns linked to the lack of expectation of privacy under the German data retention regime.[3] Systematic surveillance has a demonstrated negative effect on society, yet a limited to no demonstrated benefit.

Existing legislation, specifically the *Telecommunications (Interception and Access) Act 1979* (Cth), in part by act of omission and in part by implication, is interpreted by the executive branch and specifically by the bodies under the Attorney-General as allowing receipt of information generated as part of the act of using telecommunications products by law enforcement agencies — without the need of a warrant. This interpretation has occured without adequate consultation or public debate. Specifically, the Attorney-General's Department (AGD) has created a class of information it calls "meta-data". This ill-defined concept which the AGD has refused to give a clear outline to contains — at a minimum — all of the information available as phone records for phone conversations, including, but not limited to, information about the subscribers and (in the case of cellular communication) their approximate location and the source and destination email address of electronic mail. It is also possible to define "meta-data" in a profoundly more intrusive way — such as the web history of an individual (since it contains the web addresses visited and not their contents, it can con-

[1] Attorney-General's Department, '*Telecommunications (Interception and Access) Act 1979* Annual Report for the year ending 30 June 2012' (2012).

[2] Ibid 66.

[3] Forsa, 'Meinungen der Bundesbürger zur Vorratsdatenspeicherung' (in German) [Opinions of German Citizens on Data Retention] (Survey, May 2008).

ceivably be considered meta-data) and the subject of email messages (which, it can be argued, are capable of describing the message without being part of the contents). Lacking a substantive definition, it is not known if the AGD is considering these rather extensive interpretations.

It is important to explain what this metadata, even at its narrowest definition, actually reveals. The metadata of someone's mobile phone records, for example, provides intelligence and law enforcement agencies with what amounts to a tracking device being placed on the target over the length of time accessed by the agency. It includes who was contacted, when, and from where. If the person under surveillance has a data plan as part of their phone service, it will include email data, which, while excluding the content of the mail themselves, includes who has sent mail and any titles of the mail sent. A German Greens MP, Malte Spitz, sued his mobile phone provider for his communications metadata. Once released to him, Mr Spitz used this information to map his precise movements over a six month period, which including who he was in contact with every single day. This is a stark illustration of the data that is currently available to a myriad of Australia law enforcement and intelligence agencies without any legal oversight.[4] It is plain why law enforcement absolutely needs access to this type of information during their daily work, as it can be invaluable for conducting an investigation — Pirate Party Australia does not contest this aspect.

However, as it currently stands, the power to receive this information has been left completely at the hands of our executive branch. In a democracy such powers are traditionally assigned to the executive branch, only under the strict oversight of the legislative branch — as in any other case where two basic values conflict: the right of an individual for privacy, and the need to enforce the law and ensure our safety. In most law enforcement activities that require an intrusion of privacy, a court is involved and a warrant must be issued. Existing legislation has not speficied this need explicitly and this bill intends to correct that mistake. It is an important bill that is necessary to curtail the current use of this power. Its abuse is plain — where around 300,000 requests have been made last year, or over 800 per day. It is inconceivable that we have 800 real new suspects every day, in crimes important enough where the investigation neccesitates invading their privacy. Democracy abhors this type of abuse and this power must be put in check, lest we lose the balance between the pillars that maintain our democracy.

[4] 'Tell-all telephone', *Zeit Online* (online), no date <http://www.zeit.de/datenschutz/malte-spitz-data-retention/>.

The opposing consideration is of course that law enforcement agencies would have to spend an additional effort in requesting this warrant. In a democracy, this burden is unfortunately necessary. In the same manner that the burden existed before bursting into an individual's home, before searching an individual and before reading an individual's mail, so too the burden of having to obtain a warrant must apply when finding out fine detail on where the person is now and has been in the past, whom the person called, emailed or otherwise communicated with. Claims of an excessive burden are to be expected and these claims have to be carefuly evaluated against the democratic values of this country, which in our opinon, ultimately means they must be dismissed. The claim that warrantless access to hundreds of thousands of individuals' private data is required for government agencies to continue to do their jobs has not been backed up by evidence. Australian law enforcement agencies have, thus far, shown themselves capable of seeking and complying with warrants which have involved a degree of procedural burden. Pirate Party Australia is confident these agencies can continue this in the future, with newer technologies.

Pirate Party Australia sees no reason why the same legal safeguards that have protected our privacy for decades needs to be cast aside due to changes in technology. Therefore, we support the modest changes proposed in the Telecommunications Amendment (Get a Warrant) Bill 2013, which aim to reign in the culture of warrantless surveillance that has developed over the last decade.