Telecommunications Amendment (Get a Warrant) Bill 2013

Submission to the Senate Legal and Constitutional Affairs Committee

August 2013

Australian Privacy Foundation

email: mail@privacy.org.au

website : www.privacy.org.au

The Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For further information about the Foundation and the Charter, see www.privacy.org.au[1]

The Committee will be aware that the APF has long had an interest in the policy area of telecommunications surveillance, having made submissions and given evidence on many Bills amending the Telecommunications interception regime over the last 20 years.

Publication of submissions

We note that we have no objection to the publication of this submission in full. To further the public interest in transparency of public policy processes, APF strongly supports the position that all submissions to public Inquiries and reviews should be publicly available, except to the extent that a submitter has reasonable grounds for confidentiality for all, or preferably part of, a submission.

Introduction

We welcome the opportunity to contribute to this inquiry, but note that the failure to directly notify us of the inquiry and deadlines, despite our known interest in the policy area, has unfortunately limited our response – while we were aware of the Bill, we were only reminded of the inquiry by a media report, after the official submission deadline expired. We are grateful for the extension granted, but have only

[1] Please note that APF does not have a single postal address – we prefer communication by e-mail. If a postal address is required please contact the signatory.

had two days to compile this submission, which would have benefitted from more time and detailed analysis. We understand that several other public interest groups are in a similar position, and urge the Committee in future to proactively seek input from known stakeholders (as it has done with us in past inquiries).

This Private Member's Bill refreshingly cuts directly to a core issue underlying telecommunications surveillance law – the appropriate processes and thresholds for authorizing collection of information about the communications of Australians and others. This 'traffic data', often misleadingly referred to as 'metadata' is inherently sensitive.

This inquiry provides a valuable opportunity to debate the principles that should underly communications surveillance, free from the immediate distraction of particular government proposals for yet more changes (invariably privacy-negative to the regime.

We welcome the recognition, in the *Statement of Compatibility with Human Rights* accompanying the Bill, of the report earlier this year of the Independent National Security Legislation Monitor, and of the 2012 report of the UN Special Rapporteur. That report of course pre-dated the recent revelations about communications surveillance not only by US intelligence agencies but more generally by many governments. These revelations have prompted a long overdue debate, worldwide, about the legitimacy and proportionality of state surveillance of communications. At stake are fundamental principles of the rule of law, accountability of governments, and the balance to be struck between national security and law enforcement on the one hand and fundamental human rights and freedoms on the other, including the right to individual privacy, autonomy and dignity, and freedoms of assembly, opinion and expression which underpin democracy.

We draw the committee's attention to a recent initiative by more than 100 NGOs, around the globe, to issue International Principles on the Application of Human Rights to Communications Surveillance (https://en.necessaryandproportionate.org/text), which is a direct response to the recent revelations, but which are also based on many decades of resistance to what has appeared until now to be a remorseless rise of the surveillance state.

We also urge the Committee to consider carefully the recent report of the Parliamentary Joint Committee on Intelligence and Security's report on potential reforms to National Security Legislation (http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm), in particular its highly critical comments on the government's flimsy and inadequately justified proposals for communications data retention. Obviously the privacy impact of any traffic data access regime depends partly on the amount of traffic data held (and for how long) that is available for access at any point in time. A warrant based access scheme would be even more important if telcos or ISPs are in future to be required by law to retain more traffic data, and for longer, than they need for their own business purposes.

We cannot over-emphasise the importance of the opportunity the Committee has in this Inquiry to at least commence a re-assessment of the principles that should underly communications surveillance.

The Bill

The Bill is admirably simple in seeking to apply a general principle to all communications surveillance – that warrants, issued only after judicial oversight[2], should be required for government access to information about the communications of Australians.

The current regime for government access to information about communications rests on a foundation distinction between what used to be called 'traffic data' and 'content'. In recent public discourse, traffic data is often referred to as 'metadata'. We strongly submit that this is an inappropriate term to be used in this context. Metadata means data about data, and is most commonly used to describe aggregate characteristics of a data set, as opposed to the individual data items. In the context of open government, and maximizing the public benefit from government data, metadata is almost synonymous with de-identified data, which can be used and disclosed without any personal privacy concerns arising. In the telecommunications context, traffic data is still at the level of the individual communication – and is very often personal information that can be attributed to an identifiable individual. The Privacy Act definition of personal information has recently been amended to ensure that the Act's protections apply to information even if on its face it is not about an identified individual.

It is misleading and disingenuous for governments to classify telecommunications traffic data as mere 'metadata' as if this somehow required lesser protection and fewer safeguards

The APF supports the call in the Explanatory Memorandum for the government to implement the Australian Law Reform Commission (ALRC)'s recommendation that the Telecommunications (Interception and Access) Act (TIA Act) be reviewed in its entirety. We endorse the position that until an Australian government does so, the TIA must be amended piecemeal, such as with this Bill, to remedy specific defects.

We note that the Bill would apply the warrant regime that currently applies to stored communications and 'content' of communications to traffic data. In previous submissions on successive Bills amending the TIA Act we have drawn attention to the many ways in which even that regime has been progressively weakened. Changes have included increasing the breadth and scope of warrants, lowering the criminal offence thresholds which qualify for warrants and, very significantly, allowing warrants to be issued by designated members of the Administrative Appeals Tribunal (AAT), who are arguably not 'independent judicial officers' in the same way as judges or magistrates are (The vast majority of warrants are now issued by AAT members rather than by federal court judges).

These are matters that should be reviewed as part of the more general review of the TIA Act. For now, and in the interests of early restitution of greater safeguards, the existing warrant regime would be a major improvement on the current 'warrantless access' situation.

[2] In the case of ASIO access, the Bill accepts that warrants may be issued by the Attorney-General rather than by an independent judicial officer (the same distinction as currently applies to warrants for content of communications. In the context of recent revelations about US surveillance practices, this is arguably too generous a concession – serious questions have been raised about the adequacy of even judicial authorisation under the FISA Act, where secret warrants are routinely issued for incredibly broad and untargeted collections of communications data.

Board Members
Australian Privacy Foundation

APF Web site: http://www.privacy.org.au

Please note that APF's preferred mode of communication is by email, which should be answered without undue delay. APF does not have an organisational postal address. If postal communication is necessary, please contact the person named above to arrange for a postal address.