30 July 2013

Committee Secretary
Senate Standing Committee on Legal and Constitutional Affairs
Parliament House
CANBERRA ACT 2600

Inquiry into the Telecommunications Amendment (Get a Warrant) Bill 2013

I am making this submission in support of the Telecommunications Amendment (Get a Warrant) Bill 2013. If enacted, this bill will ensure that freedom of association, privacy and expression is not gradually eroded by warrantless access to emerging surveillance technologies which gather and analyse communications data.

The function of these technologies is often described by their proponents as "metadata collection" – a term which seeks to minimise and obscure the scope of any infringement to civil liberties. For example, we are told that the content of a telephone call is not recorded, only the time it was made, who was called, for how long, and the location of the caller.

The data stored seems minimal – merely "where", "when", and "who". However, much more can be determined by combining the gathered records and looking for patterns over time. As an example, the participants in and locations of meetings – even where meetings are currently being held – can be built up from metadata.

I am of the belief that advocates of the status quo emphasise that only metadata is subject to warrantless access in order to create a false choice between total surveillance and a curtailed version of the same. Instead, we should seek to ensure that the rights of the public are respected while serving the legitimate needs of law enforcement.

The requirement for a warrant protects the public from unjustified access to their homes and persons. More and more of the information law enforcement would seek via such access is becoming available through communications surveillance – it is therefore vital that this information be similarly protected. The government and law enforcement cannot oversee themselves; and whenever they seek to do so their legitimacy and authority can only be eroded.

The safety of whistleblowers – and their confidence in that safety – is vital to ensuring that corruption can be exposed. Warrantless access to communications data is making safe contact with the press almost impossible. If a journalist publishes an article exposing corruption in a government agency, it may be possible for the individuals responsible for that corruption to trace the whistleblower by accessing the communication records of the journalist.

Any warrantless capability to determine the location and membership of meetings could be used to curtail the actions of organised labour. It is possible to imagine that in a repeat of the 1998 Waterfront Dispute – where the government of the day supported an employer in conflict with a union – intelligence on the location and attendance of meetings could be used to harass union members and to suppress legal industrial action.

A government might attempt to justify such a misuse of gathered communications data by claiming a need to protect public safety. The unspoken assumption – that protests will necessarily be dangerous – is clearly an untruth. Judicial oversight is required to protect against such abuses and ensure that the right of employees to organise and act is preserved.

Submissions to this inquiry may assert that a requirement to obtain a warrant is excessively burdensome. I would ask the committee to observe that law enforcement in Australia is effective despite requiring warrants to access private premises. Warrants can be obtained with speed and sufficient ease. I see no evidence that a requirement to obtain a warrant before accessing communications data would adversely impact law enforcement outcomes.

Yours sincerely,

Grahame Bowland