Australian
Privacy
Foundation

http://www.privacy.org.au

http://www.privacy.org.au/About/Contacts.html

14 November 2011

Mr Hamish Hansford
Secretary
Senate Legal and Constitutional Affairs Committee
LegCon.Sen@aph.gov.au

Dear Mr Hansford

Re: Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010

Question on Notice

When I gave evidence to the Committee on 11 November, the Chair referred to the seizure of a journalist's mobile phone call records by NT Police, and asked:

> "It would be interesting to know, if this bill grants more agencies an expanded role, whether that implicates them in any of that behaviour and whether or not that is a loophole in the telecommunications act, with regard to sources of information that journalists receive via telephone, that this committee would need to look at"

With the assistrance of Mr Stephen Blanks, Secretary of NSW CCL (which you will have noted also submitted to the Inquiry), I advise as follows.

The ability of agencies to access 'telecommunications data' under the TIAA commenced on 1 November 2007. There is no need for a warrant. Access can be authorised by an officer of the agency.

In 2008-09, there were almost a quarter-million such accesses – meaning that agencies have exploited the loophole such that it has rapidly become a thoroughly routine interference with privacy. NT police make considerable use the power, although proportionately less than other jurisdictions, with 807 instances in 2008-09.

The NT incident follows a similar incident in Victoria which was reported in September:
http://www.heraldsun.com.au/news/victoria/spy-force-exposed/story-e6frf7kx-1225928598852

The relevant provision is as follows:
Telecommunications (Interception And Access) Act 1979, s.178
http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/s178.html

(2) An authorised officer of an enforcement agency may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

(3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.

Because s.178(3) is unqualfied, it allows agencies to access to telecommunications records of persons who are not themselves suspects in an investigation, and to do so without any form of judicial supervision.

The provision is seriously flawed.

It has been subjected to attack on civil liberties grounds since it was first mooted. Among other things, it does not take into account the particular privacy considerations applicable to journalists, whistleblowers etc.; and it underlines the complete unacceptability in a free nation of the replacement of judicidial warrants with agency self-authorisation.

As we understand it, the journalist shield legislation would not fix any aspect of this serious loophole, because enforcement agencies could continue to acquire such data.

In short, the argument put forward by Ken Parish at Charles Darwin University would appear to be essentially correct.

The Act currently under consideration by the Committee's Inquiry makes a very bad situation even worse, by creating yet more loopholes.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation