Submission by Guardian Australia
to the Australian Senate
Legal and Constitutional Affairs References Committee
inquiry into the comprehensive revision
of the *Telecommunications (Interception and Access) Act 1979* (Cth)

Introduction

As the Australian edition of the news organisation[1] that published stories based on disclosures by whistleblower Edward Snowden about surveillance of massive scale and questionable legality, Guardian Australia welcomes the opportunity to lodge a submission to the Committee's inquiry. For brevity's sake the *Telecommunications (Interception and Access) Act 1979* (Cth) will be referred to in this submission as 'the TIA Act'.

The TIA Act, as it currently operates and as it would operate under some proposals, presents a clear and present danger to the legitimate role journalists and their sources play in this democratic society.

Guardian Australia submits that:

- thresholds for lawful surveillance are too low
- the range of recipients of communications data is too broad
- oversight is too weak
- transparency should be increased, and that
- in light of recent disclosures the Committee should place on government agencies that conduct surveillance under law a heavy onus to regain trust through the acceptance of improved checks and balances.

[1] The relevant Guardian coverage is accessible at http://www.theguardian.com/world/the-nsa-files Key disclosures were described and put into context in a written submission by the Guardian to a UK

Key disclosures were described and put into context in a written submission by the Guardian to a UK Parliamentary Committee on 3 December 2013 – see Home Affairs Committee hearings during inquiry into counter terrorism, Guardian Media Group written submission CT 17

This submission recommends measures to help ensure that journalists and sources can operate without unjustified surveillance from government agencies or the interference that such surveillance may facilitate.

1. Warrantless access to telecommunications data poses a grave risk to public interest journalism and risks exposure of journalists' sources.

Put very simply, the TIA Act permits:

- Access under warrant to the content of real-time communications, like phone calls. whilst they are happening;
- Access under warrant to the content of stored communications, like emails, voicemails and text messages; and
- Warrantless access to metadata, which is the information generated as you use technology, but not what the contents of communications.

Guardian Australia has serious reservations about the breadth of information that can be accessed without judicial warrant and the number and type of agencies that can seek access to 'telecommunications data', also known as metadata.

The collection, use or release of the communications between journalists and their sources, without proper checks and balances, can seriously endanger journalists and their sources.

The potential for government to interfere with legitimate journalistic activity is very real if the contents of journalists' real-time or stored communications are obtained.

The Committee is urged to recommend that in any comprehensively revised TIA Act the threshold for the granting of warrants to such

communications be set at a high level, proportionate to the significance of such communications to the proper workings of a democratic society.

On this point Guardian Australia draws the Committee's attention to the analysis and revised guidelines of the United States Department of Justice – see Report of Review of News Media Policies, July 2013 – which was ordered by President Obama after misuse by US law enforcement agencies of powers akin to those of the TIA Act to investigate on journalists and their sources.[2]

In Submission 36 to this Inquiry the Australian Privacy Foundation describes what it calls 'the metadata furphy'. Metadata is not benign or insignificant because it does not comprise the actual contents of a communication. On the contrary, metadata is potent in itself. Guardian Australia endorses the APF on this point.

Metadata can expose a journalist's entire network of contacts. If collected and collated, it can create a comprehensive portrait of an individual's personal and professional life. It can show who they met, where they met and for how long they spoke. Some contacts may be sources who are seeking to alert the public - through journalists and at some risk to themselves - about matters of significant public interest. Whistleblowers are one of the key safety valves of a democratic society and the work of journalists who engage with potential whistleblowers to assess motive and verify information and its implications if it were to be widely disclosed is imperative.

The use of metadata can be even more revealing than information about content, as noted by Princeton professor of computer science and public affairs Edward W Felton:

> *Analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content…In some cases, telephony metadata can reveal information that is even more*

[2] The report is available online at http://www.justice.gov/ag/news-media.pdf

> *sensitive than the contents of the communication. (From his submission to ACLU v James Clapper.)*

Information that can be sought by agencies includes telephone numbers called or texted, time and dates of messages or calls, general location information, the length of the communication as well as email addresses and IP addresses. The names, addresses and contact information about the parties who are in communication held by the telecommunications providers can also be revealed. Guardian Australia asked one of our reporters to track what could be learnt about them from their metadata in a 24 hour period, which showed a comprehensive picture of their daily activities. The combination of this data creates a rich mosaic of information that can pose a serious threat to journalists' ability to communicate confidentially with their sources.

Through analysis of the phone numbers, frequency, times and dates and locations of calls/messages, links may be inferred between particular sources and particular stories by the journalist. Pattern recognition and other software tools make it possible to analyse vast amounts of telecommunications data in ways inimical to the maintenance of the confidentiality essential to a journalist's professional relationships.

The limited oversight of requests and uses of metadata increases the risk they will be used against journalists and sources in an impermissibly obstructive or punitive way.

Access to telecommunications data is not conditional on a warrant from a judicial authority. Authorised officers within government agencies can seek access to telecommunications data by simply applying to a telecommunications provider for access to the information. The absence of judicial oversight means that no independent authority assesses each claim for access on the merits and whether it will affect a journalist or their sources.

It is not known whether the telecommunications data which is obtained piece by piece, investigation by investigation, is combined and stored in databases for subsequent searching and matching. The potential intrusiveness of this kind of activity was vividly described in a judgment in the US District Court by Judge Richard Leon on 16 December 2013. The Committee is referred in particular to pages 44-56 of *Klayman v Obama*, US District Court, District of Columbia, Civil Action No. 13-0851.

Any comprehensively revised TIA Act needs to address with precision the issue of potential storage, search, uses and oversight of bulk metadata, or for that matter bulk contents of communications.

Agencies that can seek access to telecommunications data include those that are involved in criminal law enforcement, enforcement of a law that imposes a pecuniary penalty or the protection of the public revenue. These circumstances cover an extraordinary range of agencies, and have led to applications for telecommunications data by entities ranging from the RSPCA, local councils, Racing NSW and Roads and Maritime Services (NSW).

Requests for telecommunications data are also steadily rising. There were 319,874 applications in the 2012/2013 reporting period, an increase on the 290,358 in the 2011/2012 reporting period.

This combination of factors – breadth and power of information potentially available, range of potential recipient agencies, increasing frequency of requests – has the potential to chill activities which in a democratic society journalists legitimately pursue.

The surveillance of journalists should never be undertaken by investigative agencies of the executive without proper scrutiny by the judiciary in advance, nor without appropriate oversight afterwards by the judiciary or by suitably equipped and independent regulatory agencies.

Term of reference (a) of this Inquiry expressly requires the Committee to consider recommendation 71-2 of the Australian Law Reform Commission's Report 108 (May 2008) in which, among other things, the ALRC proposed a review of the *Telecommunications Act 1997* (Cth) and the TIA Act. In particular the ALRC recommended (at 71-2 e) that the review consider whether the TIA Act should be amended to provide for the role of a public interest monitor (PIM). One function of a PIM would be to appear before judges to test the claims of agencies seeking warrants to intercept communications. This is especially important because such applications are necessarily heard *ex parte*.

Guardian Australia supports the establishment of a PIM.

The ALRC acknowledged (at para 71.71 of Report 108) that existing oversight of agencies that intercept communications and gather metadata occurs mostly *after* a warrant has been issued. In relation in particular to applications to intercept communications or gather metadata relating to journalists and their sources, it would be an important safeguard for a PIM to be able to appear and test the grounds for a warrant *before* a judge decides whether to issue one.

The threshold for warrants to intercept journalists' communications – real-time and stored – should also be higher and warrants should be required for access to journalists' metadata.

In shaping the comprehensive revision of the TIA Act the Committee is urged to consider the 13 International Principles on the Application of Human Rights to Communications Surveillance[3] endorsed in July 2013 by a wide range of organisations from diverse countries and legal systems. The following excerpts from the proportionality principle indicate the kinds of tests which should be applied, with a PIM's assistance, to applications for warrants to intercept journalists' communications or to gather their metadata:

[3] Full text and list of signatories available at https://en.necessaryandproportionate.org/text

...if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

1. there is a high degree of probability that a serious crime has been or will be committed;
2. evidence of such a crime would be obtained by accessing the protected information sought;
3. other available less invasive investigative techniques have been exhausted;
4. information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and
5. information is accessed only by the specified authority and used for the purpose for which authorisation was given.

2. Oversight of Australia's intelligence community and enforcement agencies should be reviewed to ensure more transparency of interception activities.

The *Telecommunications (Interception and Access) Act 1979* (Cth) touches on the operation of intelligence agencies with respect to the collection of some forms of telecommunications data and interceptions. These activities are subject to oversight by the Inspector General of Intelligence and Security, State and Commonwealth Ombudsman's and parliamentary committees.

However, very limited information about the operation of these agencies is able to be released and oversight functions are spread across different organisations. The Office of the Australian Information Commissioner notes in their submissions to this inquiry that fragmentation of oversight could increase the risk of inconsistent standards in the protection of privacy. This issue applies equally to the protection of journalists and their sources.

Further, Australia's intelligence agencies fall entirely outside the scope of the *Freedom of Information Act 1982* (Cth), contrary even to current information access laws in the United States.

Telecommunications providers themselves also have significant limitations on the information they can release to the public. Greater and more consistent oversight and transparency about how intelligence agencies and

enforcement agencies are using or seeking to use the significant powers granted to them may help to deter misuse and build public trust..

The Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation 2013* recommended a review of oversight arrangements to ensure there is effective accountability under the TIA Act. Guardian Australia urges this Senate Committee to review the current oversight arrangements for communications interceptions and metadata collection with a view to a more robust scheme that ensures greater access for the public to information about the operation of the scheme.

3. Changes flagged by the Attorney General's department to force people to assist in decryption could also pose an additional threat to journalists and their sources.

Guardian Australia notes with concern a proposal by the Attorney General's department to compel telecommunications service providers or "other persons" to provide data in an intelligible format. The effect of such an order, if applied to a journalists' data, could mean that the telecommunications provider or "other persons" would decrypt information that may jeopardise the journalist's sources.

National Security Agency whistleblower Edward Snowden's disclosures of mass surveillance and bulk metadata collection have led to more journalists using a range of encryption tools to protect their sources and work practices. The use of court ordered notices to force communications service providers and unspecified third parties to decrypt data or files poses a threat to the legitimate activities of journalists, including their obligation to protect sources. We strongly urge that the Committee not adopt any proposals that could allow such a power to be exercised in relation to journalists' data without safeguards including external scrutiny and the requirement for appropriate processes to be followed before any such order could be given.

4 In light of recent disclosures, this Committee should place on government agencies that conduct surveillance a heavy onus to regain trust through the acceptance of improved checks and balances.

Guardian Australia urges the Committee to examine the activities of Australia's intelligence and law enforcement agencies. To date there has been limited constructive public debate about the role of intelligence and enforcement agencies in Australia by the appropriate overseers and ministers responsible for their administration. The scrutiny and discussion that has taken place in the US as a result of stories published based on disclosures by whistleblower Edward Snowden has not occurred in Australia.

In the US President Obama has welcomed debate, appointed an expert panel to review the issues, released the panel's report recommending reform and announced some responses to the recommendations. A similar process in Australia would be welcome.

Federal government agencies have also consistently played down the necessity for any review of surveillance powers. The Attorney General's department 2012 discussion paper 'Equipping Australian Against Emerging and Evolving Threats' ably makes a case for more surveillance, greater powers, lower thresholds and a more flexible accountability structure:[4]

> …Many of the [reporting for accountability] requirements reflect historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate.

Many of the submissions to this inquiry by various enforcement and intelligence agencies call for more powers in a range of areas. Guardian Australia urges this Committee to treat with caution any calls for greater

[4] The paper is available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm

surveillance and intelligence gathering powers under the TIA Act pending a fuller inquiry and response from Australia's intelligence and enforcement community.

We would argue that the Committee should recommend a much more rigorous system of oversight of all agencies exercising the powers of surveillance.

Katharine Viner
Editor-in-chief, Guardian Australia