**ANALYSIS:** Patrick Fair examines the state of play in varying obligations on personal data

**COVID:** Customer satisfaction holding up despite pandemic

**HOME AFFAIRS:** Future of TSSR subject of consultation

**11,951 opens last issue***

COMMUNICATIONS DAY

18 August 2020 What's happening today in telecoms ISSUE 5986

**ANALYSIS by Patrick Fair**

# The need for consistency on natsec obligations

While all attention is on the pandemic, the federal government is conducting three reviews of our national security framework which could have a long-term impact on the privacy of Australian citizens for years into the future.

One review relates to the power of agencies to get into the systems and data used for or associated with communications, contained in the so-called TOLA act. Another is the mandatory data retention regime review. The third is a review of a new law that will allow local agencies to obtain information from offshore service providers in par-

ticipating countries and facilitate reciprocal access to information held in Australia from offshore, named the International Production Orders bill. The reviews are being conducted by the Parliamentary Joint Committee on Intelligence and Security.

A key issue in each review is whether security and law enforcement agencies should be able to access IT systems and potentially, personal information without a warrant. Under the mandatory data retention regime they can; under the IPO Bill they can't without an independently issued order; and under TOLA, the intention is that they can if its metadata, but that a warrant is required for accessing information where a warrant would, but for TOLA, have otherwise been required.

TOLA is a standout because of its complexity and because it represents a paradigm shift. Instead of the agency having the power to ask for information under an authorisation or warrant and have the subject able to consider the request and comply or contest the warrant in the traditional way, TOLA gives agencies a power to obtain direct access to information on their own authorisation by making the third party do "listed acts or things". Issues with TOLA were compounded by the government introducing last minute changes that had not been previously seen or properly considered before being passed leading to an immediate further review and, most recently, a report from the Independent National Security Legislation Monitor on the merits of the legislation.

The Monitor's report endorses and supports key submissions by industry and civil society representatives to the joint committee regarding potential changes to the scheme introduced by the TOLA. The recommendations represent an appropriate rebalancing between the power of government agencies and independent operation of tech companies potentially subject to the new rules. If adopted, they would help alleviate concerns that Australian IT services and service providers cannot be trusted because they are subject to unconstrained government supervision/control.

The joint committee should adopt the Monitor's recommendations and take a wider view regarding implications of its analysis including by introducing a supervised process for access to metadata held under the mandatory data retention scheme.

The Monitor's views are based on a careful examination of the significance of the powers in TOLA and their potential implications of the scheme for secure messaging and personal privacy. In particular, the Monitor does not accept the argument that because TOLA only provides for "assistance and access" for systems - rather than access to person-to-person messages or other records or documents that might ordinarily be the subject of a warrant, often referred to as "content" as distinct from "metadata" - the broad "own motion" powers granted to agencies should be tolerated.

A pre-TOLA example of security legislation put forward and implemented with relatively light control and oversight is the data retention rules introduced in 2015. The data retention scheme is similar to the TOLA in that it also gives national security and enforcement agencies power to access metadata without a warrant and with potentially significant potential impact on a person's privacy. Agency actions are also not subject to review prior to being executed. The monitor's views on oversight, authorisation, transparency, and review should be supported but they have wider implications. In particular, they are relevant to the data retention regime and should also be considered by the joint committee in its current review of that scheme.

TOLA introduced a new Part 15 to the Telecoms Act whereby certain national security and enforcement agencies can request or require tech companies to do "listed acts or things" for law enforcement or national security purposes. Most remarkably the

companies might be required to remove a form of electronic protection, install software or equipment, provide technical information, provide access to premises or technical systems, and/or help conceal an authorised intrusion. The broad powers to get into commercial systems without independent review is not well moderated by the legal framework. For example, the power to install equipment or software can be exercised without the tech company being informed of what the software or equipment is or can do.

**THE SELF-ASSESSMENT PROBLEM:** While the government was sensitive to public concern about the potential impact on encrypted messaging (TOLA is subject to a limitation regarding the introduction of a "systemic weakness" or "systemic vulnerability") the extraordinary power to change how a system might operate, who might control the system or have visibility of the information it is processing (through the introduction of software or equipment) is limited only to a self-assessment of "proportionality". It is also significant that there is nothing in TOLA that would prevent installed software or equipment from making the data on a system directly accessible to an agency. Section 317ZH, introduced by TOLA, says that a compulsory notice issued under TOLA has no effect if it would make the subject party do an act for which a warrant would be required. This section misses the point that if software or equipment makes information directly accessible, access can be achieved without a subject party doing an act for which a warrant would be required.

As part of its considerations, the Monitor reviewed the arrangements put in place by the UK government for the exercise of similar powers introduced by the Investigative Powers Act 2016 UK.

In particular, it considered and appears to have been strongly influenced by the UK Investigatory Powers Commissioner, where a senior serving or retired judge assisted by a Technology Advisory Panel and Technical Advisory Board reviews the exercise of Powers under the IP Act including by having a power to disapprove (with reasons) the decision of a minister to issue to issue and IP Act warrant.

The Monitor's Report recommends that government agencies not have power to issue order access or control of tech systems without third party review. It also recommends clarification of the confusing language and limited scope of the definitions "systemic weakness" and "systemic vulnerability" (by deleting one and introducing clarifying examples for the other ) and raises the bar for use of the new powers so that any relevant offence being investigated must be punishable by at least seven years in prison instead of the current three years.

The Monitor recommends the creation of a new Investigatory Powers Division of the Administrative Appeals Tribunal for the purpose of deciding whether or not to issue the new compulsory orders. It is recommended that the Division consist of a new part time Deputy President of the AAT who will be an Australian Investigatory Powers Commissioner with technical and legal support. The IPC is recommended to have a role in the issue of compulsory notices under the TOLA, sharing information with other investigative bodies, managing procedures and submission from entities subject to orders and reporting annually on the operation of to the Attorney-General and the Parliamentary Joint Committee on Intelligence and Security.

The Monitor makes these recommendations even though the TOLA is focussed on "assistance and access" rather than content. He says "...I do not accept that 'a key safeguard in [the relevant powers] is that they cannot authorise access to data', access be-

ing granted by separate warrant issued by a tribunal member or judge. This argument elevates form over substance..."

The Monitor does not go into the debate over whether "content" is more significant than metadata from a privacy perspective, focusing instead on the highly coercive nature of the powers. He could have made much more of this issue.

The debate over content vs metadata famously entered the public arena when in October 2014 then Attorney-General George Brandis played down the significance of digital meta-data as the "name and address on the envelope." In a digital environment, metadata is much more than the addressee and (possibly the sender) published on the outside of an envelope to the postal service. Under the regime, it includes the name of the user, the device they are using, the service they are using, the source and destination of a communication, the type of communication, the date time and duration of a communication, the location of the device used to make the communication. This information was never on the outside of an envelope. Our regime allows for it to be requested prospectively and be provided as a form of surveillance.

Under the regime it can be obtained for any period within the previous two years or prospectively. In 2018-19, 291,353 requests were made, including 27,824 prospective authorisations for criminal law enforcement. Metadata is more privacy-intrusive than most content because it is factual and, particularly when taken over time, can indicate likely location, contacts, activities, relationships, and imply lifestyle and beliefs.

The Monitor's report has been published at a time when the IPO Bill has been tabled in Federal Parliament and is also being reviewed by the Joint Committee. The IPO Bill creates a procedure for Australian agencies to obtain meta-data and/or content from foreign tech companies but only if the International Production Order is approved and issued by an eligible judge or member of the AAT Security Division. The Monitor observes that the proposed role of the Tribunal in the issue of IPOs is consistent with its recommendations. It is notable that the role of the Tribunal in the issue of IPOs is inconsistent with the agency self-authorisation regime that applies to access to metadata. The IPO Bill will put in place AAT supervision of international production orders for obtaining metadata and content from offshore providers even though a similar requirement does not apply for access to metadata held locally.

The Joint Committee is considering the Monitor's report and is currently undertaking further hearings. Its recommendations should be supported. The Joint Committee should also consider the bigger picture by taking the Monitor's observations into account in its reviews of the IPO Bill and MDR regime. While it is necessary and desirable to give government agencies the powers, they need to carry out national security and law enforcement responsibilities efficiently, we should have a consistent approach to the protection of personal information. In particular, the Joint Committee should recognise that the self-authorisation scheme that facilitates high volume access to metadata under the Data Retention regime is out of place and recommend that it be brought in line with the IPO Bill and the Monitor's recommendations on TOLA.

**Patrick Fair, adjunct professor at the School of Information Technology, Faculty of Science, Engineering and Built Environment at Deakin University, is the principal of Patrick Fair Associates, the chairman of the Communications Security Reference Panel at Communications Alliance, and general advisor for LexisNexis Practical Guidance Cybersecurity, Data Protection and Privacy.**