December 2021

UPDATE

Major overhaul of Electronic Surveillance, Anti-Trolling Bill and developments in Security of Critical Infrastructure

1. Electronic Surveillance Reform Discussion paper

On 6 December 2021 the Department of Home Affairs released a Discussion Paper, *Reform of Australia's electronic surveillance framework*. The discussion paper asks for feedback regarding a new electronic surveillance law to replace the existing *Telecommunications (Interception and Access) Act 1979* (**TIAA**), *Surveillance Devices Act 2004*, Part 15 and potentially is Part 14 of the *Telecommunications Act 1997* and replace (or override) State Acts dealing with listening and tracking devices.

The discussion paper references issues identified by the Richardson Report (see our Update 6), inconsistencies within the federal law and between state laws.

Feedback sought relates to wide range of fundamental issues, including:

- What information should be accessible by law enforcement and national security and how should it be shared and used?
- Who should be able to access information? The paper suggests expanding the electronic surveillance powers of AUSTRAC and other agencies.
- What private sector service providers will be required to conduct data collection and surveillance? The existing interception regime institutionalises interception systems within regulated telecommunications companies and some obligations apply more broadly. The paper proposes to expand the regulation to cover communications providers whether or not they provide telecommunications services.
- How should agencies be authorised to gain lawful access to information? The discussion paper asks whether the existing warrant framework (for content) and own motion notice framework (for metadata) remains suitable including who should have authority to grant rights of access.
- Comment is sought regarding the implications that might arise from use of artificial intelligence and attribute-based warrants (i.e., surveillance of a class rather than targeted collection of information relating to an identified individual)
- General feedback is sought regarding safeguards, oversight and reporting.
- Feedback is also sought regarding the practical operation of the existing system and ways it might be improved.

The discussion paper includes a list of official enquiries and reports relating to electronic surveillance indicating that Home Affairs intends to take them into account.

Comment:. The proposed reform is a timely reset of a complex and outdated legal framework. Obvious potential improvements might include: introducing a coherent, principles-based framework; better accountability and supervision of law enforcement and national security agencies; clear obligations on agencies to publish timely, detailed and relevant information regarding the use and effectiveness of surveillance powers and the activities of supervisory agencies; a comprehensive framework to protect information once collected; include a framework to protect journalists and whistle-blowers with comprehensive coverage; an ability for parties obliged to facilitate interception and data disclosure to inform their users regarding the nature and extent of the surveillance taking place; reset of the highly dubious

official position (as legislated in the TIAA) that access to metadata is not sufficiently privacy intrusive to require a warrant; more transparency and suitable control of large scale surveillance and use of data analytics, and implementation of the recommendations of the Independent Security Legislation Monitor regarding the powers in Part 15 of the Telco Act (knows as the Encryption Bill).

More likely, the new framework will expand the powers of law enforcement and national security agencies and create new compliance obligations and costs for data collection and delivery for services associated with information management. You can access the consultation page here. Submissions close on Friday 11 February.

2. Consultation on new Online (Anti-Trolling) Bill.

On 1 December 2021, the federal government commenced consultation on a Bill with potential to expose social media companies and businesses trading in personal information to liability for defamation arising from comments posted by Australian located users of the service subject to certain conditions.

Liability is imposed by:

- Deeming the regulated party to be a primary publisher and, thereby, removing the innocent dissemination defence.
- In the case of social media companies who would also be "internet content hosts" within the meaning of the Broadcasting Services Act, removing the defence in section 91 of Schedule 5 of the *Broadcasting Services Act 1992*.

The Bill provides regulated entities with a defence if they obtain identity information relating to each of their users and identify the maker of an offending post to an aggrieved party, court or regulator.

Comment. The explanatory note associated with the exposure draft of the legislation explains that the legislation in part responds to the decision in *Fairfax Media Publications v Voller [2021] HCA 27* (**Voller**). However, the Voller decision did not impact the defence in the Schedule 5 of the *Broadcasting Services Act 1992* which is removed for the purposes of the Bill. By deleting the BSA defence the scheme proposes to an important liability protection for social media platforms as an incentive for collecting, maintaining and, when required, disclosing user details.

Information regarding the consultation is available here. Submissions close 21 January 2021

3. Developments in Security of Critical Infrastructure.

The amendments to the *Security of Critical Infrastructure Act 2018* (**Act**) referred to in our last Update as Bill 1 received Royal assent on 2 December 2021. A consolidated version of the Act incorporating the changes in available here. An exposure draft of Bill 2 has been published and is open for consultation until 1 February 2022.

The Minister has made Rules narrowing the scope of some asset definitions used in the Act. The Rules implements the position described in the scope of coverage discussion paper published in April 2021 without change.

The Department of Home Affairs has begun consulting on the Ministerial Instrument that will specify the critical infrastructure assets that must comply with ownership, operation and cyber incident reporting obligations. The regulation allows a three-month sunrise period for meeting the cyber security incident reporting obligation and a six-month sunrise for ownership and operational reporting. The consultation period closes 1 February 2022. Details are available here.

Please contact me if you have any questions regarding the matters discussed in this update.
patrick@patrickfair.com 0411361534

You can subscribe to updates like this one at www.patrickfair.com