PiperAlderman

Article Information

Author: Tim Clark
Service: Intellectual Property & Technology
Sector: IT & Telecommunications

The new data retention laws – what should you be aware of?

The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth) (otherwise known as the "new data retention laws")

The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth) (otherwise known as the "new data retention laws") has been passed into law in April 2015. ***Partner, Tim Clark*** *and* ***Lawyer, Philip Chow****, provide a concise summary of the new laws and how they may affect your business.*

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (Act) amends the existing *Telecommunications (Interception and Access) Act 1979* (Cth) to require service providers operating a "relevant service" (Service Providers) to retain "metadata" for a minimum period of two years. "Relevant service" principally covers telecommunications and internet service providers, who have until 13 October 2015 to comply with the main operative provisions.

The key provisions

Under existing laws, many law enforcement agencies already have access to certain "metadata" without the need of a court warrant. Authorised Officers of an enforcement agency can request Service Providers to disclose specified information or documents by way of a written authorisation. Service Providers must provide "such help as is reasonably necessary" for purposes such as safeguarding national security and the enforcement of criminal laws and laws imposing a pecuniary penalty. However, Service Providers are not mandated generally to retain any particular "metadata", nor to retain it for any particular period of time. Any information that is retained is at the Service Provider's discretion. Law enforcement agencies have identified the lack of data availability as a key impediment in some criminal investigations.

The Act aims to address this issue by requiring Service Providers to retain "metadata" for a minimum period of 2 years. Although the main provisions of the Act commences later this year, compliance with the data retention requirements may be deferred for up to a further 18 months if Service Providers submit, and have approved, a data retention implementation plan by 13 October 2015. This transition scheme allows Service Providers to design their own pathway to reach full compliance with the Act. There are substantial civil penalties for the failure to comply with the data retention implementation plan (and thereafter, the obligation to retain "metadata" pursuant to the Act).

The types of "metadata" that must be retained are specified in the Act. Broadly, it includes:

- identification information about the account holder (e.g. name, address or billing information)
- information about the source and destination of a communication
- date, time and duration of a communication
- type of communication (e.g. voice, SMS or email) or the type of relevant service used for a communication (e.g. ADSL, wifi, VoIP or cable)
- location of equipment or line used at both ends of a communication.

Apart from the specified types of "metadata," the Act grants the Minister broad powers to add or amend the list through a declaration by legislative instrument, which are only effective for 40 parliamentary sitting days. Permanent changes must be effected by legislative amendment that has been reviewed by a parliamentary joint committee for not less than 15 parliamentary sitting days.

The Act retains the existing procedures for accessing stored "metadata". However, the range of enforcement agencies that are able to access the information are now limited to a specific list of "criminal law – enforcement agencies." The effect of

this change remains to be seen as the Minister has power to declare an agency to be a permitted enforcement agency if, amongst other considerations, the Minister is satisfied on reasonable grounds that the authority is a law enforcing body.

How does it affect you if you are not a telecommunications or internet service provider?

From a reading of the Act, private internal networks and public wifi could be considered a "relevant service" that is required to comply with the data retention obligations. However, the Act provides two limited exemptions to prevent these services from falling within scope.

First, services that are "provided only to a person's immediate circle" are excluded. This is intended to exempt internal networks operated by government departments, tertiary education institutions or large corporations from data retention obligations. However, the protection does not cover networks offered to persons outside of the "immediate circle". The definition of "immediate circle" is limited to persons specified in section 23 of the *Telecommunications Act 1997* (Cth). By way of example, tertiary education institutions must limit access to their internal networks to individuals who are a member of the governing body, an officer, an employee or a student.

Second, the Act excludes a service that is provided only to places that "are all in the same area." This clause is intended to exempt cafes and restaurants providing free wifi access from compliance with data retention laws. Instead, the obligation to retain "metadata" rests with the internet service provider, supplying the underlying internet service.

The above exemptions, however, have their limits. The Communications Access Co-ordinator has power to impose the data retention laws on any particular service despite the exemptions. Organisations will also need to have adequate procedures and policies to ensure access to their internal networks are appropriately limited, failing which, they will have data retention obligations under the Act. Finally, whilst a tertiary education institution, government department or corporation might not be required to retain "metadata" in relation to their internal networks, these bodies invariably rely on external telecommunications and internet services provided by Service Providers, who are mandated to store the "metadata." This has important implications for these organisations as enforcement agencies will have access to substantial amounts of "metadata" that could reveal a lot about an organisation's activities.

One important implication is that, although the Act clarifies that "metadata" is not to be disclosed or used in relation to civil proceedings, information about civil contraventions might inadvertently be published through enforcement activities. Further, some activities may potentially involve both criminal offences and civil contraventions. For example, "metadata" could reveal widespread downloading of copyright-infringing material in a university's or government department's networks in the course of a criminal investigation. An enforcement agency may, during its investigations, disclose that fact despite no criminal conduct being found. This could alert potential civil litigants to seek discovery in relation to an organisation's computer systems or logs. Ultimately, the Act provides greater scope for an organisation's activities to leave an evidentiary trail that could be used against it in regulatory investigations as well as potentially encouraging civil litigation.

Conclusion

The Act does not generally impose any data retention requirements on an entity that is not a telecommunications or internet services provider. However, organisations operating internal networks need to ensure that their networks are exempted under the Act. Otherwise, they will need processes to comply with the new data retention requirements. In any event, legal compliance policies of organisations should be reviewed to ensure that they are adequate to minimise legal compliance risks in circumstances where evidence of non-compliance may be more readily available in regulatory investigations or which may encourage civil litigation.

Piper Alderman would be pleased to assist your organisation in understanding the requirements for compliance with the Act, as well as reviewing legal compliance policies and programs to identify if there are areas of compliance risk requiring attention. For assistant, contact Tim Clark or a member of our IP, Telecommunication & Technology.