Published on *The National Law Review* https://natlawreview.com

Australia's New Mandatory Data Retention Law

Article By:

Courtney M Bowman

Last week, Australia became the latest country to pass a mandatory data retention law. The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015, which amends Australia's Telecommunications (Interception and Access) Act 1979, requires telecommunications and Internet service providers (ISPs) to store customer metadata for two years. This means that Australian ISPs and telecom providers will have to store data associated with electronic communications, such as the names and addresses of account holders, the names of the recipients of any communications, the time and duration of communications, the location of equipment used to make the communication (such as cell towers), and computers' IP addresses. Although the law does not require ISPs and telecoms to store the contents of customers' electronic communications, metadata still can provide a picture of an individual's identity, interests, and even location, which makes it of great interest to law enforcement and national security agencies seeking to prevent crime and terrorist attacks. Indeed, the law was promoted as a national security measure designed to give law enforcement access to information that could allow them to prevent terrorist attacks, but its opponents have decried it as a means to subject Australians to mass government surveillance.

As in Australia, laws that require ISPs and telecoms to retain customer metadata have proven controversial the world over, and some have been struck down by courts. In 2014, the Court of Justice of the EU struck down the EU's 2006 Data Retention Directive, which mandated that member states enact laws requiring telecoms and ISPs to store customer metadata for the benefit of law enforcement, because it found the Directive violated Europeans' fundamental right to privacy. Likewise, the Supreme Court of Argentina struck down that country's mandatory data retention law as unconstitutional in 2009. However, the UK's Data Retention and Investigatory Powers Act 2014 (DRIP) remains in force. It should be noted that although the United States currently does not have a similar federal data retention law, the Electronic Communications Privacy Act of 1986 permits law enforcement to request the preservation of and/or access certain types of stored data if specific conditions are met.

Regardless of the controversy mandatory data retention laws tend to generate, ISPs and telecoms should be aware that similar laws are in effect (or may eventually take effect) in a number of jurisdictions around the world, and that they may be expected to comply with these laws. They should also be aware that their storage of customers' metadata – which could be construed as personal data or personally identifying information in some jurisdictions, given the amount of information it can provide about a person's identity and whereabouts – also implicates privacy concerns. Accordingly, if

a company is subject to a mandatory data retention law, it should ensure that any data it is required to retain is stored securely so as to mitigate the possibility of a breach or other violation of relevant privacy laws.

National Law Review, Volume V, Number 91