RETENTION

Professor Urges Second Look at Push for Expanded Metadata Laws

Granting law enforcement more powers in accessing metadata is an Australian trend that troubles at least one law professor. Rick Sarre, of the University of South Australia, writes on *TheConversation.com* that the push to allow authorities to access encrypted digital data has consequences that must be considered.

Angus Taylor, minister for Law Enforcement and Cybersecurity, said the government will continue to pursue new powers that permit authorities access to encrypted metadata in the fight against terrorism, organized crime, and online crime.

Sarre, in response, encourages a review of the record in this trend of granting increased access to metadata. He writes that 21 law enforcement agencies have been granted access to track and retain metadata. "Given the ubiquity of smartphones and other portable devices, these agencies can find an enormously rich trail of information on users' locations, calls, and networks."

In 2015, new laws required telecoms to retain and store their metadata for two years so that it would be available for analysis. At the time, the government sought to ease concerns about "overreach" by granting more power to the Commonwealth Ombudsman to monitor compliance.

Sarre writes that a primary concern was that the new laws would "erode the very democratic freedoms that governments are duty bound to protect, such as freedom of political association." He cites an April 2017 incident in which an Australian Federal Police operative sought and acquired the call records of a journalist without a warrant.

Lost, perhaps, in the traditional privacy concerns was the likelihood that this strategy was not future-proof. Technologies that conceal metadata from collection are already rampant, he asserts. "Any encrypted messaging app — such as Wickr, Phantom Secure, Blackberry, WhatsApp, Tango, Threema and Viber — can circumvent data retention. Moreover, any secure drop system based on Tor is capable of evading metadata scrutiny too."

Minister Taylor, aware of this reality, therefore seeks to continue pursuing new powers. Sarre asks, "Will this be through some form of commercial arrangement? Will it be via a threat to block services of non-compliant telcos? Will it involve embedding surveillance codes in devices? Will warrants be required in all cases? How much will it cost?"

The professor goes on to question whether the current metadata laws are having any effect. He says there is anecdotal evidence now and again, but no actual confirmed evidence that access to metadata has disrupted any threats to national security. In turn, he offers this caveat: "It is worth remembering that governments must ensure that no policy sacrifices our hard-fought liberties in the pursuit of an expensive goal that is not readily attainable."

FOIA

FOIA Backlog Is Trimmed Even as Requests Set Record

As reported on *FedWeek.com,* U.S. federal agencies received a record 818,271 requests under the Freedom of Information Act in fiscal 2017, according to the Justice Department, but agencies still managed to reduce the backlog to just more than 111,300 by processing 823,222.

The total number of requests has risen steadily from roughly 600,000 in fiscal 2010. Currently, the Department of Homeland Security continues to account for the largest share, at 45%. The departments of Justice and Defense and the National Archives and Records Administration accounted for 10%, 7%, and 7%, respectively.

According to the article, about 22% of the requests were fully granted, 37% partially granted, 22% had no relevant records found, 5% were denied based on exceptions under law, and the rest were withdrawn, duplicative, or had other outcomes.