Australian Government
Attorney-General's Department

Data Retention Facts

Keeping our community safe – Fact sheet

The Australian Government is committed to providing our law enforcement and security agencies with the tools they need to keep our community safe by requiring the telecommunications industry to retain a limited set of metadata for two years.

This will be supported by existing as well as important new oversight and accountability mechanisms to protect the privacy of Australians' personal information.

What is metadata?

On 30 October 2014, the government introduced the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014. The Bill will require Australian telecommunications companies to keep a limited set of telecommunications data ('metadata') for two years, which will be defined in regulations. The Bill passed the Parliament on 26 March 2015 and received Royal Assent on 13 April 2015.

Metadata is information about the circumstances of a communication (the who, when and where)—not the content or substance of a communication (the what).

For phone calls, metadata is information like the phone numbers of the people talking to each other and how long they talked to each other—not what they said.

For internet activity, metadata is information such as an email address and when it was sent—not the subject line of an email or its content.

Why is metadata critical for our law enforcement and security agencies?

Metadata is vital to nearly every counter-terrorism, organised crime, counter-espionage and cyber-security investigation. It is used in almost every serious criminal investigation, including murder, sexual assault, child exploitation and kidnapping.

This type of data is valuable to help:

- promptly identify suspects and exclude people from suspicion—innocent people can be ruled out as a suspect without having to be subjected to more invasive investigations
- support applications to use complex and intrusive tools, such as a warrant to intercept the content of communications
- provide evidence in prosecutions.

Why do we need a data retention regime?

Changes in business practices and developments in technology mean that many telecommunication companies are no longer retaining some types of metadata, or are not retaining it for a useful period of time for law enforcement and national security agencies to investigate and prosecute serious crimes. As a result, Australia's law enforcement and national security agencies have advised that their investigative capabilities are at risk of being significantly degraded.

The two year retention period is based on advice from law enforcement and security agencies. The most serious and complex cases, such as terrorism, espionage, organised crime, financial crime and public corruption, involve lengthy investigations. There are also many crimes, such as sexual assault, which are often not brought to the attention of authorities until long after they occurred.

Telecommunications companies will have up to two years to fully implement the scheme. To prevent any further erosion of metadata, industry will be required to at least maintain their current practices for holding data during the implementation period.

What kind of metadata will be kept?

The government is asking Australian telecommunications companies to keep for two years a limited set of metadata. This is **not** the content of the communication, and web-browsing history is specifically excluded from the scheme.

The set of metadata required to be retained is defined by reference to the following six types of information: the identity of the subscriber to a communications service; the source of the communication; the destination of the communication; the date, time and duration of the communication; the type of the communication; and the location of the equipment used in the communication.

The data set is enshrined in the legislation and was developed in consultation with industry. An Implementation Working Group will continue to support implementation of the scheme. This group includes representatives from industry and government.

What safeguards and oversight arrangements will be in place?

The new scheme does not provide law enforcement or security agencies any additional powers, or give them any new capacity to access metadata.

A warrant is still required before an agency can access the content of communications.

Importantly, the reforms will significantly limit the range of agencies that are permitted to access metadata.

The Commonwealth Ombudsman will be given powers to inspect access to, and the use of, metadata by Commonwealth, state and territory enforcement agencies to ensure their compliance with relevant legislation.

A new warrant regime will apply to agencies seeking to access data about a journalist’s source. The regime includes provision for submissions by an independent Public Interest Advocate.

The Inspector-General of Intelligence and Security (IGIS) and the Privacy Commissioner will also have oversight of the operation of the data retention regime. Parliament will also play an important role through

the PJCIS and the Parliamentary Joint Committee on Law Enforcement. The Attorney-General will be required to report annually on the operation of the scheme.

What protections are in place to ensure the security of personal information?

The protection of the privacy of Australians' personal information is essential. The existing protections under the Privacy Act and Australian Privacy Principles (APPs) will continue to apply to personal information held by industry under their data retention obligations. The Privacy Commissioner will continue to assess industry compliance with the APPs, as well as monitoring industry's non-disclosure obligations in relation to telecommunications information under the Telecommunications Act.

The government will introduce reforms to strengthen the security and integrity of Australia's telecommunication infrastructure by establishing a security framework for the telecommunications sector. This will better protect information held by industry in accordance with the data retention regime. The government expects this reform will be finalised before the end of the data retention implementation period.

How much will this cost?

The Attorney-General's Department engaged PricewaterhouseCoopers (PwC) to cost the implementation of the proposed data retention regime in consultation with industry. PwC estimated the upfront capital cost of the regime to all of business to be between $188.8 million and $319.1 million, which is less than 1 per cent of the $42 billion in revenue generated by the telecommunications industry annually. This estimate will inform the Australian Government in delivering on its commitment to make a reasonable contribution to the capital costs of implementation of the data retention regime.

How does this align with international approaches?

More than 35 Western countries worldwide have legislated data retention schemes. For example, the UK Parliament has recently passed legislation to require industry participants to retain metadata.