Consumer Fact Sheet

Facts about the Federal Government's data retention scheme

The Federal Government's data retention scheme, enacted in March 2015, will come into effect between 13 October 2015 and 12 April 2017. Our fact sheet covers what consumers need to know.

What is metadata?

Metadata, simply put, is 'data about data'. In telecommunications it is information about communications (e.g. the time a phone call was made and its duration), information about the people communicating (e.g. the sender and the receiver) including account and location information, and the device used. The scheme requires that service providers retain metadata but not the content or substance of a communication. However metadata can still reveal a lot of information about an individual and those they interact with.

The set of metadata that will be required is set out in the legislation – see http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/Dataset.pdf

How will your metadata be used?

It will be mandatory for telcos and ISPs to store your metadata for two years (some may have a business need for longer retention of some data). This metadata will be available to specified government agencies (such as law enforcement and national security agencies) upon request.

You will be able to access your own data and many service providers do some of this already in your ordinary bill.

How will it affect consumers?

Costs

We don't know how much a data retention scheme will cost to set up but in March the Government estimated it at $400 million to set up and $4 per year, per customer to run. It is expected that service providers will recover these costs through a combination of Federal government funding and an increase in charges to consumers. However, the Federal budget announced in May only showed planned Government contributions to be $131 million over 3 years, with no contribution to ongoing operating costs. Therefore it is likely that your monthly phone and internet bill will increase as a result.

Consumers will have the right to access data about themselves under the Privacy Act 1988. Service providers cannot charge for an application for access, but may charge a reasonable fee for providing access. Telstra has indicated it will charge nothing for recent data as part of the standard billing

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer advocacy organisation

Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

information, but for more detailed or longer term information they will charge according to how long it takes them to compile this information. We are yet to understand what the typical fee may be.

Securing your data

Once data retention comes into practice, you will need to keep your information secure. Your service provider may provide you with a password to access your own metadata: it is essential this be kept safely as metadata will reveal much about you. *All of the devices on your account* will also be included, so this can include your partner's, children's, extended family members', employees' and so on. Whoever uses the equipment listed against your account will be included. This means if you pay for your partner, friend or elderly parent's phone and it is listed as part of your account, then you will have access to it. Correspondingly, they will have access to your metadata if they are the account holder.

This may be especially important if you are a victim of domestic violence or other predatory behaviour and your account is under someone else's name, such as your partner's, and if you feel that this may be a problem, you should make arrangements for a separate account.

ACCAN is currently working with the NSW Women's Legal Service to improve the guidance material available to women's refuges and community legal workers on this topic.

Data protection

Service providers will be required to notify you if your data is accessed unlawfully - whether provided accidentally by the service provider to a third party or through illegal access (hacking).

The legislation requires that the data be encrypted, but does not specify any particular encryption or security standard to be complied with.

Which businesses will be included?

Businesses defined under the Broadcasting Services Act (1992) as carriage service providers will have to retain data on customer usage. Any internet service provider and telecommunications carrier operating in Australia is included. This means the Australian based companies that provide you with telephone services or internet access.

Which businesses are not included?

Only Australian telecommunications businesses are included, companies providing telecommunications services from overseas are not included. If you are planning to avoid this legislation by using overseas providers, note that these companies are also not subject to other Australian regulation (or privacy safeguards) so may not work as you expect, either. This could be as simple as using a different dial tone, to not reaching emergency services with 000, or charging you according to ways we normally expect in Australia. Companies registered in Australia are listed in ASIC's database.

Many people access the internet from their place of employment and most Australian workplaces are not 'carriage service providers', so aren't included. Universities, schools and colleges are for the most part not included either because they are generally not defined as 'carriage service providers'. However the network that connects between universities, colleges and schools (AARNet) is, so some data will be retained.

Calls and internet access made from hotels, internet cafés, coffee shops and shopping centres will not generally be subject to this legislation, but their service providers will be. For example, using a Telstra Wi-Fi service regardless of where it is located is included, and coffee shops selling Telstra services with their own brand on the front will be included. Coffee shops providing Wi-Fi using their own equipment will not be included.

Companies that provide you with services *over* the internet are also not included, such as Google (including Gmail and Google Drive), Facebook, Skype, WhatsApp, Viber, Wickr, Yahoo!, Tumblr, Flickr, Instagram, Pinterest, LinkedIn, Gumtree, and eBay.

Transition, exemptions and variations.

The legislation provides for service providers to submit a 'data retention implementation plan' for a staged introduction of the retention requirements, which must however be complete by 12 April 2017. There is also provision for application for exemptions and variations from the requirements. Decisions on these applications are made by the Communications Access Co-ordinator (and official in the Attorney-General's Department) with review by the Australian Communications and Media Authority (ACMA). However, applications and decisions will be confidential, so consumers will not know when, and to what extent, their service provider is bound by the requirements.

Which agencies can access metadata without a warrant?

- Australian Federal Police
- State Police Forces
- Australian Commission for Law Enforcement Integrity
- Australian Crime Commission
- Australian Customs and Border Protection Service
- Australian Competition and Consumer Commission
- Australian Securities and Investments Commission
- Crime Commission (NSW)
- Independent Commission Against Corruption (NSW)
- Police Integrity Commission (NSW)
- Independent Broad-based Anti-corruption Commission (Victoria)
- Crime and Corruption Commission of Queensland
- Corruption and Crime Commission (WA)
- Independent Commissioner Against Corruption (SA)

The Federal Attorney General may also add additional agencies with parliament's approval.

Is this a new power?

This scheme does not give a new power to access metadata. However, the data set which service providers will have to keep will be consistent, and the minimum data retention period of two years will be mandatory for all service providers unless they are granted an exemption or variation. In the past, the range of data kept by service providers and the time they kept it for was different for each organisation.

Previously, any government agency able to impose a fine was able to request metadata, and over 80 agencies did so in 2012-13. However, not all service providers would always provide it to all agencies. Under the data retention scheme the number of agencies able to access metadata without a warrant will be restricted.

The legislation establishing the scheme is the ***Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015***

Further information about the Data Retention Scheme can be found at:
http://www.ag.gov.au/NationalSecurity/DataRetention/