Submission No 227

Inquiry into potential reforms of National Security Legislation

Organisation: Australian Security Intelligence Organisation
Australian Federal Police
Australian Crime Commission

Supplementary Submission to PJCIS: ASIO, AFP and ACC

Data Retention

26 October 2012

Contents

Data Retention 3
What is telecommunications data? 3
Current Access Arrangements – What we do now 4
Proposed Reforms 4
Accountability 5
Attachment A: Data Retention: Frequently Asked Questions 6
Why does this information need to be retained? 6
There is no proof that data retention is needed. 7
For how long do agencies want the data retained? 7
What will data retention cost? 7
Is it possible to separate communications data and content? 7
Isn't data retention just a way of seeing everyone's browsing history? 8
Will purpose-built facilities be required to store the large volumes of data? 8
Should agencies require a warrant to access telecommunications data? 8
How will the retained data be protected from unauthorised access? 8
Why does Australia want data retention when it has been found unconstitutional in Germany? 9
Why are we only looking at the EU for a data retention model? 9
How has the EU DRD been implemented across the EU? 9

Data Retention

This paper explains the operational imperatives of ASIO, the AFP and the ACC, behind the data retention proposals under review by the PJCIS. It has been prepared as an unclassified document to allow the Committee the discretion to publish the contents if desired, with a view to clarifying some of the public misconceptions regarding the proposed national security reforms. This includes confirming that ASIO, the AFP and the ACC do not want the internet browsing history of every customer of an internet service provider (ISP) to be retained.

What is telecommunications data?

Also known as metadata, communications data and communications associated data, this data relates to communications for telephones (fixed and mobile) and the internet and falls into two categories:

Category 1: Information that allows a communication to occur:

- The internet identifier (information that uniquely identifies a person on the internet) assigned to the user by the provider[1];
- For a mobile telephone service: the number called or texted;
- The service identifier used to send a communication, for example the user's email address, phone number or VoIP number (internet telephone number);
- The time and date of a communication;
- General location information, for example mobile telephone cell tower; and
- The duration of the communication.

Category 2: Information about the parties to the communications is information about the person who owns the service. This would include:

- The name and address of the customer;
- The postal and/or billing addresses of the customer (if different);
- The contact details, mobile telephone number, email address and landline phone number of the customer; and
- The same information on the recipient party if known by the service provider.

Telecommunications data does not include the content of communications.

[1] Internet identifier is a reference to Internet Protocol (IP) addresses or an IP address and port number. An IP address is a unique string of numbers separated by periods that identifies each computer attached to the internet. Some networks also use an additional number called a port number to expand their allocation of IP addresses.

Current Access Arrangements – What we do now

At present, for the conduct of their lawful functions, ASIO, the AFP and the ACC rely extensively on telecommunications data already held by telecommunications providers.

Part 4-1 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) already empowers agencies to authorise disclosure of information required for investigative purposes. Agencies are currently able to access the data described above, upon appropriate authorisation, provided the service providers have retained the data and it is in an accessible form.

However, one of the key difficulties driving the requirement for data retention is the speed with which the business model of telecommunications providers is progressively moving towards billing arrangements based on data quantities rather than individual calls or communications. This can result in providers no longer retaining call or message histories of vital importance to understanding the extent and nature of contact which may be of security concern.

- For example, with the popularity of pre-paid telephones, mobile phone providers do not necessarily need to keep details of every call made for their own business purposes. Instead, they may only need to keep information about the duration (and subsequent costs) of each call.

Another difficulty is the nature of internet connections, where the unique internet identifier assigned to an individual (roughly the equivalent of a phone number) can change with each login. This means that data retention would require the ISP to keep a record of who was assigned a particular IP address at a specific time.

- ISPs inconsistently retain this information for their own business purposes and hence this information, which is essential to investigative efforts and public safety, will be lost.

Proposed Reforms

Currently neither the TIA Act nor the *Telecommunications Act 1997* define telecommunications data. As a result, the regularity and accessibility of telecommunications data retained by service providers varies considerably.

ASIO, the AFP and the ACC are seeking amendments to the TIA Act to make the legislation technologically neutral, in particular:

- clarify the description of what telecommunications data should be retained for law enforcement or security purposes in accordance with the description of telecommunications data above; and

- require telecommunications and internet service providers to retain such data for a specified period in a form that is readily accessible by agencies under appropriate authorisations.

This will address the key need for clarity and consistency across industry as to which telecommunications data will be retained and for how long.

Accountability

There has been substantial media reporting alleging the lack of accountability around the access to this type of data by agencies like ASIO, the AFP and the ACC.

ASIO, the AFP and the ACC recognise the need for and value of comprehensive and stringent accountability and governance mechanisms for all operational activities. Requests for data prepared to date by each agency have been, and will continue to be, carefully scrutinised by appropriately senior officers to ensure a direct need for the data in the context of an investigation, an appropriate level of threat, imminence or seriousness, and a clear correlation to the functions of the agency involved.

The Commonwealth Ombudsman provides oversight of law enforcement compliance with aspects of the TIA Act. ASIO has the specific oversight provided by the Inspector-General of Intelligence and Security (IGIS). ASIO, the AFP and the ACC advocate the continuation of the existing comprehensive and appropriate accountability, oversight and reporting arrangements.

Attachment A: Data Retention: Frequently Asked Questions

Why does this information need to be retained?

Telecommunications interception and access to telecommunications data are critical investigative tools for ASIO, law enforcement and the ACC. Almost every ASIO investigation and a large number of serious crime investigations by law enforcement agencies are assisted by some form of telecommunications data.

- In particular, telecommunications data generally enables agencies to establish the time, general location and subscriber details of telecommunications activity.
- This data is essential for the majority of investigations. Loss of access to such data, for technical or legal reasons, would result in a loss of a fundamental investigative capability and the ability of security and law enforcement agencies to function effectively.

Developments in communication have seen individuals increasingly using mobile communications and the internet (both email and internet-based phones) as their primary method for contacting others. Individuals of security interest are no different.

Mobile and internet-based communications have emerged as an important communication method for extremists, including the active and conscious use of methods to attempt to avoid the scrutiny of security and law enforcement services. Equally, the emergence of cyber espionage shows how modern technology can be used as a new vehicle for carrying out traditional espionage activities.

The following two examples illustrate the critical importance to investigations of data that increasingly may not be retained:

- Example 1: We receive intelligence that a particular IP address in Australia had been in contact with a known terrorist or criminal organisation. To determine who that user was we would need to ask the ISP involved which of their customers they allocated that IP address to at the time of the contact.
- Example 2: ASIO receives intelligence that a particular IP address is subject to cyber attack. ASIO would need to identify who that IP address is assigned to before it could warn them that their computer has been taken over and their information stolen, and to commence working with them to improve their IT security.

National security and law enforcement investigations into serious and potentially imminent threats to life are increasingly hampered by the changing business models of telecommunications providers.

- Should data retention not proceed, the problems of data access will only increase as more and more communications use internet technology.

There is no proof that data retention is needed.

Should data retention not proceed, we anticipate that almost every security intelligence and serious crime investigation undertaken by ASIO, the AFP and the ACC (and by State Police) will be affected. Telecommunications data forms the foundation for almost every serious investigation and is a significant element of the evidentiary process.

As an international example, the German Federal Police (BKA) published an analysis report[2] on the impact of their Federal Constitutional Court's decision to overturn their domestic data retention laws.

For how long do agencies want the data retained?

From an operational perspective, ASIO, the AFP and the ACC would like telecommunications data to be retained by telecommunications providers for as long as possible. There are a range of other policy considerations justifiably influencing the minimum retention period that may be specified.

The European Union Data Retention Directive (EU DRD) has been used as an example set of requirements for discussion in Australia.

What will data retention cost?

Agencies acknowledge mandatory retention of telecommunications data will impose an additional financial cost to either industry, Government or both – particularly in respect of some internet related services. This must be measured against the significant public benefit derived from data retention.

The potential impost in respect of traditional telephony is likely to be much less than for internet-related services as much of telephony data is already retained for business and taxation purposes.

We understand that implementation of the EU DRD has been neither as costly, complex or as time-consuming as originally estimated by the European industry. Australian agencies and industry should be able to benefit from the data retention solutions developed in the EU.

Previous discussions with the telecommunications industry in Australia have shown there to be a high degree of variability in costs and storage estimates. It is somewhat premature to speculate on costs at this time.

Is it possible to separate communications data and content?

Some commentary asserts that some "data" is actually content, for example some URLs (web addresses) may contain sensitive information such as usernames or passwords. There are also claims of difficulty in separating communications data from content.

[2] This report highlights that during a 13 month period without data retention, 98% of the BKA's requirements for internet subscriber details could not be met due to the data not being retained. http://www.bka.de/nn_234028/SharedDocs/Downloads/DE/ThemenABisZ/Mindestspeicherfristen/120130StatistischeDatenerhebungMindestspeicherungsfristenAbschlussbericht.html

Agencies are **NOT** seeking the retention of content or web browsing history of all Australians. ASIO, the AFP and the ACC are requesting the retention of information consistent with that in the EU DRD. Separation of content from data has not been an issue in the EU and the suggestion it is not possible to separate data and content is not consistent with information and feedback we have received from industry vendors.

Isn't data retention just a way of seeing everyone's browsing history?

No. Agencies do **NOT** want the browsing history of every customer of an ISP to be retained. While there might be significant intelligence value in accessing the web history of specific targets, this is not part of the national security reforms for the retention of telecommunications data as described above.

Critically, the TIA Act does not permit the disclosure of the contents or substance of a communication without a warrant. Agencies are not seeking any changes to this.

Will purpose-built facilities be required to store the large volumes of data?

ASIO, the AFP and the ACC are requesting information similar to that which has been retained by telephone companies for billing and tax purposes for many years and to which agencies have had access. We are not aware of purpose built facilities previously being required to store this information and understand from discussions with most of industry that these will not be required.

Anecdotal estimates before the inquiry regarding retention of IP address allocations are that this information can be stored "...a very long time at very little cost". It is noteworthy that the per unit cost of storage is decreasing worldwide.

Should agencies require a warrant to access telecommunications data?

Data authorisations are already subject to various but equally rigorous and stringent accountability regimes. Access to telecommunications data is considerably less intrusive than access to content for which a warrant is required.

To require a warrant would be expensive, logistically challenging and extensively affect police and intelligence agency investigations. There would also be a significant change to our criminal justice system and the relationship between police, intelligence agencies and the judiciary. Data access is also often only a preliminary investigative step and may in fact be used to exclude an individual from investigation. Warrants for access to telecommunications data would be unworkable.

How will the retained data be protected from unauthorised access?

Some data, including personal information such as subscriber details, is already collected and retained by industry. The protection of this data remains paramount and is one of the main drivers behind the proposed Telecommunications Sector Security Reform which aim to increase the level of security in telecommunications networks.

In addition, National Privacy Principle 4 requires that an organisation take reasonable steps to protect the personal information it holds from misuse, loss and from unauthorised access, modification or disclosure.

Why does Australia want data retention when it has been found unconstitutional in Germany?

The EU DRD has not been found unconstitutional in any jurisdiction with all 27 member states transposing the Directive into domestic law. .

Germany, Bulgaria, Romania, and the Czech Republic had their domestic data retention legislation overturned as it exceeded the requirements of the Directive and therefore the domestic laws (not the directive) were found to be unconstitutional. Bulgaria has since enacted new laws and both the Czech Republic and Romania have legislation in their parliaments. It is unclear when Germany will re-transpose the Directive and the EU Commission has initiated infraction proceedings. The German Constitutional Court did observe that it was possible to transpose the Directive in way that was consistent with the German Constitution.

Why are we only looking at the EU for a data retention model?

The European Union (EU) Data Retention Directive (2006/24/EC of 15 March 2006), is currently the only international model for data retention. The EU Directive imposes an obligation for providers of publicly available electronic communications services and public communication networks to retain communications data for the purpose of the investigation, detection and prosecution of serious crime, as defined by each EU Member State in national law.

The Directive requires the retention of subscriber and traffic data. There is no obligation on retention of the content of the communication. The Directive was developed after the London and Madrid terrorist bombings and as a response to law enforcement and national security investigative needs. Norway, a non-EU state, has also adopted the EU DRD as a model.

In May 2011, the USA introduced the Protecting Children from Internet Pornographers Act of 2011. The Act requires some providers to retain, for a period of at least 12 months, all records or other information relating to the identity of a user of the Internet. We are watching the passage of this Act with interest.

How has the EU DRD been implemented across the EU?

The EU Data Retention Directive has been implemented differently across the EU member states, with the most notable difference being who pays for the storage and access of the data. For example, the UK Government pays all costs associated with data retention, whilst in Ireland the industry bears all the costs.

There are also differences in retention periods within EU member states.