



**THE HON NICOLA ROXON MP
ATTORNEY-GENERAL
MINISTER FOR EMERGENCY MANAGEMENT**

12/7195

Anthony Byrne MP
Chair
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600
AUSTRALIA

Dear Mr Byrne

Anthony,

I refer to our meeting of 13 September 2012 and to the data retention proposal contained in my Department's discussion paper entitled "Equipping Australia Against Emerging and Evolving Threats". The Terms of Reference of my referral to the Committee state that the Government is expressly seeking the views of the Committee on a "tailored data retention scheme for periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts".

I appreciate the Committee's desire to receive further details on what this proposal may entail. I do not have a specific data retention model in mind but I can provide the following further information to clarify the parameters of this proposal.

"Telecommunications data" is information about the process of a communication, as distinct from its content. It includes information about the identity of the sending and receiving parties and related subscriber details, account identifying information collected by the telecommunications carrier or internet service provider to establish the account, and information such as the time and date of the communication, its duration, location and type of communication.

The Government does not propose that a data retention scheme would apply to the content of communications. The content of communications may include the text or substance of emails, SMS messages, phone calls or photos and documents sent over the internet. Access to the content of communication is only ever carried out under warrants issued in accordance with the *Telecommunications (Interception and Access) Act 1979*. There is no intention to alter the requirement for warranted access to the contents of communications.

The need to consider a data retention scheme has come about because of changes in technology that have affected the behaviour of criminal and national security suspects. Targets of interest now utilise the wide range of telecommunications services available to them to communicate, coordinate, manage and carry out their activities. The ability to

lawfully access telecommunications data held by the telecommunications industry enables investigators to identify and build a picture of a suspect, provides vital leads of inquiry and creates evidence for alibis and prosecutions.

Two examples that have been provided to my Department by State agencies serve to illustrate the importance of maintaining access to telecommunications data:

- a) During a recent murder investigation there were a number of open lines of inquiry. When a human source provided information implicating a particular, previously unknown, person as responsible for the murder, telephone billing records were used to link the person nominated by the human source to another key suspect. The billing records also ultimately resulted in other lines of enquiry being discounted. The link between two of the principal offenders could not have been easily made without access to reliable telecommunications data. All the persons involved in that matter have been charged with the murder and associated offences and are currently before the courts.
- b) A corruption investigation revealed evidence of SMS communications between a police member and a member of an organised criminal network. Despite knowledge of the communications occurring recently, no data relating to the communications was available. The inability to obtain relevant information about the communications led to the loss of evidence which could have supported the investigation into the corrupt links.

In the past the telecommunications industry retained most types of telecommunications data. However, due to rapid changes in the technology and business environment Australian agencies are finding the much of the information they seek is not being kept. The main drivers are the increased use of internet protocol technology and the trend to charge customers based on volume of data sent or received rather than by transaction (such as call by call or message by message).

Australia is not alone in being forced to consider answers to these challenges. In recognition of the impact the lack of access and retention of telecommunications data is having on investigations, the European Union adopted the EU Directive 2006/24/EC on data retention on 15 March 2006. The Directive has been implemented by the majority of the 25 Member States of the EU with the remaining Member states at various stages of implementation.

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 Member State in national law. The Directive only requires the retention of subscriber and traffic data. No data revealing the content of the communication may be retained under the Directive. The data set is at **Attachment A**.

The Directive applies to fixed network telephony (landline), mobile telephony, internet access, internet email and internet telephony. The Directive specifies that certain categories of data must be retained, namely data necessary for identifying:

- a) the source of a communication;
- b) the destination of a communication
- c) the date, time and duration of a communication;

- d) the type of a communication;
- e) users' communication equipment or what purports to be their equipment; and
- f) the location of mobile communication equipment.

The Directive requires Member States to ensure that data is retained for periods of between six and 24 months. Because there is flexibility in the Directive's requirement the EU members have picked varying retention periods appropriate for their own local needs. There is also variability in the retention period for different types of information, for example, requiring telephony data to be held for 12 months but internet data for six months.

To protect the integrity of retained data, the Directive requires Member States to ensure that operators respect four data security principles, specifically, that the retained data shall be:

- a) of the same quality and subject to the same security and protection as those data on the public communications network;
- b) subject to appropriate technical and organisation measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
- c) subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and
- d) destroyed at the end of the period of retention, except those that have been accessed and preserved for the purposes set down in the Directive.

The reasons for the implementation of the EU Directive are explained in the preamble to the Directive as a response to terrorist attacks in Europe (particularly, the Madrid and London bombings), the maintenance of ability to fight crime and terrorism and for the consistency and completeness of regulation across the EU.

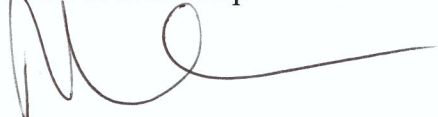
For Australia, the principal argument in favour of a data retention scheme is to maintain our agencies' access to a critically important source of intelligence and evidence. Agencies have indicated that the need to access this information is immediate and that the eroding of such access is already seriously affecting agency investigations.

I understand that the AFP will be appearing before the Committee and they will be in a position to provide details of the operational requirements for a potential data retention scheme in Australia.

I thank the Committee for its work on this and the other matters that I have referred for your consideration and I look forward to obtaining your advice on what you would consider to be an appropriate data retention scheme in Australia.

Given the high level of public interest in this inquiry I intend to make this further correspondence to the committee, public.

Yours in friendship



NICOLA ROXON

Encl : Attachment A – EU Directive on Data Retention data set

Article 5 of the EU Data Retention Directive

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.