Submission No 213

Inquiry into potential reforms of National Security Legislation

Organisation: Pirate Party Australia

Pirate Party Australia

National Security Inquiry Supplemental Submission

By Simon Frew.

With the clarifications of the data retention proposals provided by both ASIO and Attorney-General, Nicola Roxon, Pirate Party Australia would like to make a supplementary submission directly addressing the new information. While there are many other issues that have yet to be explained in any detail, we appreciate any clarification of these proposals.

From Ms Roxon's letter:

> *"Telecommunications data" is information about the process of a communication, as distinct from its content. It contains information about the identities 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.*[1]

"Telecommunications data" as defined by The Hon. Ms Roxon states that information about the process of a communication is distinct from its content. While telecommunications data may not include the content of any communication online, it can make that information accessible.

The clarification of the definition of metadata goes some way to explain what exactly is being proposed to be kept. From the ASIO submission:

> *In the context of TI reform "data" or CAD generally refers to information about communications – not the actual substance or content of those communications. For example: phone number xxxxxxxxxx called number yyyyyyyy at 10:00 on 12 September 2012; not what was said during the conversation.*[2]

This is currently accessible by intelligence agencies without any need for a warrant. Pirate Party Australia reiterates its opposition to agents of any Australian intelligence or security organisation having access to Australians' private data (even metadata) without judicial oversight.

According the ASIO the data retention regime 'may' include:

> *- data to identify the parties of a communication;*
> *- data to identify the origin and destination of a communication;*
> *- data to identify the date, time and duration of a communication;*
> *- data to identify the type of communication (eg. phone call, email)*

---

[1] The Hon. Nicola Roxon MP. **Letter clarifying Data Retention Proposal.** http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/letter%20from%20ag%20to%20pjcis%20clarifying%20tor.pdf

[2] Australian Secret Intelligence Organisation **Inquiry into potential reforms of National Security Legislation** Submission No. 209. http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs/sub%20209.pdf

- data to identify users' communications equipment; and
- data to identify the location of parties to the communications.
In this context, agencies are not seeking access to the content of communications.[3]

There is no explanation as to how this would happen in regard to tracking communications. There is not a direct correlation between the operation of a telephone and the Internet so the analogy is weak and confusing. It seems that CAD is what Nicola Roxon refers to as traffic data.

Traffic data (or CAD) aims to include the sender and recipient of every communication. In the online context this would include a user's web-browsing history. To do this the metadata collected would necessarily include either the IP (Internet Protocol) address or the domain name (E.G. http://www.pirateparty.org.au/) of every website visited by every computer user in Australia.

An IP address is a number (EG 172.16.254.1) which computers use to connect to networks like the Internet. This is the computer equivalent of a web address. Domain Name Servers (otherwise known as DNS) carry out the function of converting domain names into IP addresses in the same way looking up a phone book for someones name would yield their telephone number. IP addresses can be used in web-browsers the same way as domain names.

To access the content of the website an agent only has to feed either the IP address or the domain name into the address bar of any web browser. So while only metadata is being collected, it does grant ASIO the ability to monitor everything seen by every user in Australia without a warrant.

The effectiveness of such surveillance is questionable to say the least. Most people use web-based email services (like Gmail or Hotmail) which run as encrypted connections. Any time a connection is pre-fixed with https:// instead of http:// the connection is secure. It is good practice for everyone to encrypt email communications as emails can contain sensitive personal and financial information that could be life destroying if it got into the wrong hands.

The use of encrypted email services ensures that ISPs would be unable to monitor any communications occurring within the webmail systems. The Email data that ASIO claim would be so useful in building cases just could not be stored by the ISP collection regime.

There is an array of methods to further encrypt online activities, such as Virtual Private Networks, Proxies and Tor. These hide which websites are visited, and anyone using one of these services would, for the purposes of the proposed data retention regime, be invisible.

From the clarifications offered by both the Attorney-General and ASIO it seems that there is indeed a plan to monitor every website visited by every Australian. This is nothing like having a list of phone numbers called by a suspect, it is more like having an ASIO agent seeing every news story you read, every TV show you watch and every issue you research.

When the data retention regime was implemented in Germany there was a demonstrated chilling effect on people's use of the Internet due to the perceived privacy invasion of having every interaction online tracked by spy agencies. There was also a reduction in the ability of German security agencies to solve crime with a marked reduction in the prosecution rates after data retention was implemented. This seems to be the result of too much additional

---

[3] Ibid.

information being available which can slow down and hamper investigations.[4]

This data will be held by ISPs who do not have a good record of protecting data (see our main submission for details). The risk to the private data of every Australian is too great for the scheme to be implemented. The proposal being put forward has already sparked a movement across society to learn how to keep communications private through encryption. Parties called Crypto-Parties have been held across Australia with hundreds of people already learning to avoid the surveillance methods proposed in the Inquiry. There is a very high level of interest and there will be many more of these events in the future because people who value their privacy will do whatever they can to defend it from overbearing authorities.

Ms Roxon cites the European Union's adoption of the data retention directive (Directive 2006/24/EC) as justification for the need of similar measures in Australia, writing that it "has been implemented by the majority of the 25 Member States of the EU with the remaining Member states at various stages of implementation."[5]

What Nicola Roxon fails to acknowledge is that in three member states – Germany[6], Romania[7] (where the parliament has passed it again despite the ruling) and the Czech Republic[8] – it has been declared unconstitutional. This was due to the infringement of privacy associated with such retention measures. Additionally, Sweden and Serbia have only implemented data retention for six months, not the two years the Government's discussion paper proposes.

In conclusion, the clarified data retention proposal would amount to a systematic invasion of every Australians' privacy. The claim that it would reveal useful information for intelligence agencies does not fit the facts due to the most basic encryption thwarting attempts to reveal the sought after data. The risk of the collected data being stolen from ISPs, leaked or otherwise exposed poses a threat to the security, not only of individuals, but of the country.

The serious social costs of the loss of privacy and subsequent risks to the private data of all Australians are not balanced out, by any measure, by any increased abilities in the capacity of intelligence agencies. If the German statistics bear out elsewhere, data retention actually hinders more investigations than it helps and should be rejected outright for the good of both Australia and its citizens.

---

[4] Vorratsdatenspeicherung. **Data Retention Effectiveness Report.** 2006. http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf

[5] Roxon. Op Cit.

[6] European Digital Rights. In EDRI-Gram 8.5 March 2010. http://www.edri.org/edrigram/number8.5/german-decision-data-retention-unconstitutional

[7] Ibid. Issue 10-10 23 May 2012. http://www.edri.org/edrigram/number10.10/romanian-parliament-adopts-data-retention-law-again

[8] Library of the US Congress. **Czech Republic: Constitutional Court Overturns Parts of Data Retention Law.** 2011 http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205402601_text