SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS
AUSTRALIAN FEDERAL POLICE

Question No. 233

Senator Xenophon asked the following question at the hearing on 24 February 2014:

This series of questions relates to the Surveillance Devices Act 2004 and the Telecommunications (Interception and Access) Act 1979.

1. Please provide the number of authorisations made under sections 178, 179 and 180 of the Telecommunications (Interception and Access) Act 1979 over the past three calendar years.
2. How many of these authorisations were made in the context of investigations into S. 70 and S. 79 of the Crimes Act? (suspected unauthorised disclosure of government information – so called 'leak inquiries')
3. Ford Motor Company USA has stated (3rd Feb 2014 letter to US Senator Al Franken) that it stores all GPS location data created by the cars it makes (rental and private) for 2-3 weeks, then sends it off to Acquity Group brand management company and then to other agencies. What is the situation in Australia? How is Australian GPS data collected or stored?
4. What legal authorisation is required for police to get access to GPS data of vehicles (rental and private)?
5. How does the process work? (How do your investigators actually go about getting the data?)
6. Do you have to obtain the GPS location data for individual cars as required for an investigation or do you acquire this information en masse from somewhere? And if so where?
7. How does this process work? Do you obtain GPS data from car companies in the case of private cars or rental companies for rental cars or some other way?
8. How long is GPS data stored?
9. What about GPS data in GPS devices that aren't built into cars? Eg Tom-Tom or Navman or other GPS devices you can buy off the shelf?
10. Who stores it? How is it stored? En masse in real time or specific devices as required for an investigation?
11. What legal authorisation is required for police to get access to it?
12. In relation to Interception Capability Plans, which outline how carriers and nominated carriage service providers can help law enforcement agencies with lawful interception of telecommunications services: do these plans vary significantly from company to company?
    a. Are these Interception Capability Plans available for viewing by the public?
    b. Does the Parliamentary Joint Committee on Intelligence and Security have access to these plans?
    c. Does IGIS have access to these plans?
13. How do Australian authorities go about requesting overseas carriers and carriage service providers for information about Australians?
    a. Which Treaties govern this process?
    b. How many times has this occurred in the past five years, and to which foreign countries?
    c. Please provide the number of surveillance device warrants issued under the Surveillance Devices Act 2004.

14. How many warrants were issued in the context of investigations into S. 70 and S. 79 of the Crimes Act? (suspected unauthorised disclosure of government information – so called 'leak inquiries')
15. How many times has an eligible Judge or nominated AAT member declined to issue a warrant?
16. What is the difference between a carrier and a carriage service provider?
17. In the last three calendar years, how many members of the Federal Parliament have been the subject of surveillance pursuant to the Surveillance Devices Act 2004 and/or the Telecommunications (Interception and Access) Act 1979 in the context of investigations into sections 70 & 79 of the Crimes Act (suspected unauthorised disclosure of government information - so called 'leak inquiries')?
    a. In the last three calendar years, how many authorisations have been issued against members of the Federal Parliament pursuant to the Surveillance Devices Act 2004?
    b. In the last three calendar years, how many authorisations and/or warrants have been issued against members of the Federal Parliament pursuant to the Telecommunications (Interception and Access) Act 1979 in the context of investigations into sections 70 & 79 of the Crimes Act (suspected unauthorised disclosure of government information - so called 'leak inquiries')?

The answer to the honourable senator's question is as follows:

1. Reporting is undertaken by financial year. The figures for the financial years are:
   2010/2011 – 23 351
   2011/2012 – 23 001
   2012/2013 – 25 726

2. The AFP is required to report to the Minister on the total number of authorisations made under Sections 178, 178A, 179, 180A, 180B, 180C and 180D by an authorised officer of the AFP during a particular year as per Section186 (1) of the *Telecommunications (Interception and Access) Act 1979*.

   Under the legislation, the AFP is not required to report specifically on authorisations made for investigations into particular offences, including those identified in this question, relating to S70 and S79 of the *Crimes Act 1914* (Cth).

   To comply with legislative requirements all authorisations are recorded in an AFP electronic storage system. This system is configured to record and store information contained in the authorisation and to produce reports on the total number of authorisations. Whilst the information is stored in the system, the system is not designed to report on particular crime types which are being investigated.

3. Whilst the AFP has no visibility of the Ford Motor Company's GPS data collection practices, if GPS data is collected by a vehicle or a rental agency in Australia, the AFP would be required to obtain a search warrant in order to obtain/seize the historical GPS data.

4. Where the AFP has reasonable grounds to suspect there is (or will be) evidential material on the premises, an AFP member may apply to a magistrate for a search warrant under s3E of the *Crimes Act 1914* (Cth). If issued, the warrant is executed in

accordance with the relevant provisions of the *Crimes Act 1914*, including s3F, relating to search and seizure.

5. Refer to the answer to question 4.

6. If GPS data is collected by a vehicle or rental agency, a search warrant is required to obtain/seize the historical GPS data. This information is not routinely collected en masse. Surveillance device legislation in the various jurisdictions requires a warrant or authorisation to collect live GPS data.

7. The AFP does not acquire live GPS data without a warrant or authorisation under the *Surveillance Devices Act 2004*.

8. The AFP does not know how long GPS data is stored by companies.

9. The AFP does not know how long GPS data is stored by companies.

10. The AFP does not know of the methods that particular private companies employ to collect and/or store GPS data.

11. Refer to the answer to question 4.

12. The AFP does not administer ICPs. This question should be referred to the Attorney-General's Department (AGD).

13. This question should be referred to the Attorney-General's Department (AGD).

14. No warrants can be issued under Section 70 as offences under Section 70 of the *Crimes Act 1914* (Cth) carry a maximum term of imprisonment of two years. For a telecommunications intercept warrant to be approved under the *Telecommunications (Interception and Access) Act 1979* (Cth) the offence being investigated must fit the definition of a 'serious offence' as defined under Section 5D.

    Some offences defined within Section 79 of the Crimes Act 1914 relating to 'Official Secrets' are captured within the definition of a 'serious offence'. Under the *Telecommunications (Interception and Access) Act 1979* Annual Report each year the Attorney General's Department publishes the categories of offences under which interception warrants have been issued. The AFP is not required to report specifically on particular warrants issued for investigations into particular offences. However, if warrants were issued under Section 79 they would fall within the 'Bribery and Corruption' category in this report. The AFP can confirm that in the 2012/13, 31 telecommunications interception warrants have been issued for offences under this category which also includes offences against sections 131.1, 135.1, 142.1, 142.2, 148.2 or 268.112 of the *Criminal Code Act 1995.*

    In relation to both Sections 70 and 79, the AFP is unable to disclose more specific information in relation to authorisations or warrants issued under the *Telecommunications (Interception and Access) Act 1979*.

15. In 2012/13, six applications for telecommunications interception warrants were refused. In 2012/13, four applications for surveillance device warrants were refused.

16. The *TIA Act* uses the definition from the *Telecommunications Act 1997*,

- Carriers are persons who own a telecommunications network unit to supply carriage services to the public.
- CSPs use a telecommunications network unit to supply carriage services to the public.

Carriage services include services for carrying communications, for example telephone services, Internet access services and Voice over Internet Protocol (VoIP) services.

17. The AFP is unable to disclose specific information in relation to authorisations or warrants issued under either the *Telecommunications (Interception and Access) Act 1979* or the *Surveillance Devices Act 2004*.