Annex 15: THE LAW OF THE FIVE EYES (8.41 above)

Australia

1. The primary statute governing access to intercept and communications data in Australia is the TIA 1979.[20] It is long and complex.

2. It distinguishes between "*interception*" of communications that are passing through a telecommunications system and "*access*" to stored communications on a carrier's equipment, although both are only lawful when carried out pursuant to a warrant. Interception is narrowly confined to "*real time*" communications: "*listening to or recording by any means, such a communication in its passage … without the knowledge of the person making the communication*."[21] Once a communication has become accessible to the recipient, it is no longer passing over a telecommunications system and must be accessed via a stored communications warrant.[22]

Interception

Australian Security Intelligence Organisation

3. The TIA 1979 Part 2-2 sets out the mechanism by which ASIO (the Australian equivalent of MI5, governed by the Australian Security Intelligence Organisation Act 1979) might be issued with a warrant to intercept communications. ASIO cooperates with the Australian Secret Intelligence Service **[ASIS]**, the Australian Signals Directorate and the Australian Geospatial-Intelligence Organisation.

4. ASIO may apply for, three types of warrant to intercept communications in order to access the communications of a person who is reasonably suspected of being engaged in or likely to engage in activities prejudicial to security.[23] Each of those warrants may be issued by the Attorney-General on request by the Director-General of Security:

   (a) A warrant that specifies the telecommunications service likely to be used by a person engaged in activities prejudicial to security;[24]

   (b) A named person warrant that grants authority to intercept the various communications methods employed by an individual (all their mobile phone numbers or email addresses);[25]

   (c) A B-party warrant, which enables the interception of a service that will be used by a non-suspect to communicate with a suspect.[26]

---

20 The Surveillances Devices Act 2004 and the Telecommunications Act 1997 contain further relevant provisions.
21 TIA 1979 s6(1).
22 TIA 1979 s5F(1). If only the telecommunications data is required, then stored material may be accessed without a warrant under s 178 and 179 of TIA.
23 TIA 1979 s9(1).
24 TIA 1979 s9(1).
25 TIA 1979 s9A.
26 TIA 1979 s9(1)(a)(ia).

5. Accordingly, national security warrants may only be obtained for quite narrow purposes; they do not provide a basis for bulk interception. Section 10 sets out a mechanism for the issuing of emergency warrants, when the Director General of Security considers it appropriate, for no longer than 48 hours.

6. A separate regime governs the grant of warrants where ASIO wishes to intercept "*foreign intelligence"*. In each case, the Attorney-General must be satisfied, on the basis of advice from the Minister of Defence or Foreign Affairs, that obtaining the foreign intelligence set out in the notice is in the interests of Australia's national security, foreign relations or economic well-being. Once again, three types of warrant may be issued:

   (a) A warrant authorising interception on quite a general level to a particular "*telecommunications service*." Where known, the name and address, occupation and number of the subscriber should be set out in the request.[27]

   (b) A named person warrant, for which the application must specify the telecommunications service that is being used by a person or foreign organisation and the foreign intelligence information that will be obtained.[28]

   (c) A "*foreign communications*" warrant for the interception of foreign communications only, (those sent or received outside of Australia.[29]

7. The Director-General must not request the issue of a foreign intelligence warrant under s 11A, 11B or 11C for the purpose of collecting information concerning an Australian citizen or permanent resident.[30]

Law Enforcement Authorities

8. The TIA 1979 Part 2-5 sets out the circumstances in which law enforcement bodies may intercept telecommunications. They may apply for a warrant to an eligible Judge or a nominated member of the Administrative Appeals Tribunal **[AAT]**. A range of agencies can apply, at both the state and federal level, including the Independent Broad-based Anti-Corruption Commission and various Crime Commissions.[31]

9. The application must be supported by an affidavit setting out the facts and other grounds on which it is based. Two types of warrant may be issued:

   (a) A telecommunications service warrant, which authorises the interception of a particular telecommunications service that may be used by an identified individual. It must set out the number of previous applications (if any) related to the service or that person and the use made by the agency of information obtained by interceptions under those warrants.

27 TIA 1979 s11A(1).
28 TIA 1979 s11B.
29 TIA 1979 s11C.
30 TIA 1979 s11D(5).
31 TIA 1979 s39.

(b) A named person warrant, which must set out the name of the person and details sufficient to identify the telecommunications service they are using, details of previous applications and use made of the material obtained.[32]

10. The Judge or AAT member must be satisfied that there are reasonable grounds for suspecting that a particular person is using or is likely to use the service and the information that would be likely to be obtained would be likely to assist in connection with the investigation by the agency of a serious offence.

11. The Judge or AAT member should have regard to:

(a) How much the privacy of any person or persons would be interfered with;

(b) The gravity of the conduct constituting the offence;

(c) The value of the information obtained;

(d) The extent to which other methods have been used, would be likely to assist, or might prejudice the investigation.

12. They must be satisfied that all other practicable methods of accessing the communications have been exhausted.[33]

13. Warrants may be sought and obtained, in urgent circumstances, via telephone.[34]

Stored Communications

14. The TIA 1979 Part 3 contains a separate regime governing access to stored communications. In broad terms, both ASIO and criminal law enforcement agencies are entitled to issue preservation notices, requiring a carrier to preserve all stored communications specified in the notice.[35] The notice may only specify one person or telecommunications service.[36] The TIA 1979 distinguishes between a domestic preservation notice and a foreign preservation notice. A foreign preservation notice is issued when a foreign country intends to request the Attorney-General to secure access to telecommunications. In that sense, they reflect the UK's MLAT regime.[37]

15. ASIO does not have to apply for a preservation notice before seeking access to material on the basis of a warrant. It may apply for a warrant in any case where it reasonable grounds for suspecting that a particular carrier holds stored communications that is likely to assist in connection with the investigation of a serious contravention (a crime of sufficient seriousness).[38] Furthermore, ASIO does not normally have to apply for a separate stored communications warrant. An interception warrant will also entitle them

32 TIA 1979 ss42 and 46A.
33 TIA 1979 ss46 and 46A.
34 TIA 1979 ss43 and 50.
35 Recent changes have added a new TIA 1979 s110A that has restricted the power to access stored telecommunications data to "*criminal law enforcement agencies*", rather than the broader law enforcement agencies described above.
36 TIA 1979 s107H(3).
37 TIA 1979 s107N.
38 TIA 1979 s106(c).

to access stored communications if the warrant would have authorised interception if it were still in passage.[39] However, a criminal law enforcement agency will need to apply for a stored communications warrant.

16. TIA 1979 contains a number of provisions relating to the destruction of material obtained via warrants.

Telecommunications data

17. TIA 1979 Part 4 sets out the circumstances in which bodies may obtain access to telecommunications data. Telecommunications data is not formally defined, although it does not include the contents or substance of a communication.[40] A new mandatory data retention regime specifies categories of information that must be kept by service providers for a period of two years.[41] These categories include the subscriber of a relevant service and the source, time, date, and location of a communication.[42]

18. Sections 174-6 provide for three types of disclosure of telecommunications data to ASIO. Firstly, on a voluntary basis by a service provider "*if the disclosure is in connection with the performance by* [ASIO] *of its functions*." Secondly, an authorisation for access to existing information or documents (which may be granted by the Director General of Security, Deputy Director General of Security and an officer of ASIO approved by the Director General). Thirdly, a slightly wider body of individuals may authorise access to prospective information (anybody above a certain level of seniority within ASIO may grant permission), for not longer than 90 days.[43] In the case of an authorised disclosure, the authorising individual must be satisfied that the disclosure would be "*in connection with the performance by* [ASIO] *of its functions*".

19. Sections 177-180 set out the framework governing the disclosure of existing telecommunications data to enforcement agencies (which includes any criminal law enforcement agency). An enforcement agency may authorise the disclosure of telecommunications data where reasonably necessary to enforce the criminal law, locate missing persons, enforce a law imposing a pecuniary penalty or protect the public revenue. Accordingly, bodies that have the power to levy a fine may seek access to telecommunications data.[44] The disclosure of prospective telecommunications data may be authorised for a limited period where reasonably necessary for the investigation of a serious offence.[45]

20. Sections 180A and 180E allow authorised officers of the Australian Federal Police to obtain access to telecommunications data for the purpose of further disclosing that material to a foreign authority. The procedure, as with intercepted material, is similar to the UK's MLAT process.

---

39 TIA 1979 s109.
40 TIA 1979 s172.
41 TIA 1979 s187C.
42 TIA 1979 s187A.
43 TIA 1979 ss175-6.
44 As long as they are defined as an enforcement agency in the newly amended TIA (see s110A).
45 TIA 1979 s180.

21. Before any authorisation is made (on any of the bases set out above) the authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with privacy is justifiable and proportionate.[46]

22. An authorisation, the notification of that authorisation, revocation and notification of the revocation must be in written or electronic form, and must contain:

    (a) The identity of the eligible person and the basis on which they are eligible to make the authorisation;

    (b) The person or company from whom the disclosure is sought;

    (c) Details of the information or documents to be disclosed;

    (d) A statement that the eligible person considers that to be in connection with ASIO's functions; and

    (e) The date of the authorisation. [47]

23. Authorisations made on behalf of an enforcement agency must set out certain additional material. The rules are very detailed and vary, depending on whether the material is historic or prospective and on behalf of a foreign government or not.

24. Each year, the head of an enforcement agency must give the Minister a written report that sets out the number of authorisations made and the number of disclosures to foreign countries and names of those countries. The minister consolidates that material and lays before Parliament a report that sets out the consolidated material.[48]

The Australian Secret Intelligence Service

25. Different provisions apply to the activities of ASIS (the equivalent of MI6), which are controlled by the Intelligence Services Act 2001 **[ISA 2001]**.

26. ASIS may gather intelligence about an Australian person or class of Australian persons outside Australia, as long as this is authorised by the Minister for Foreign Affairs.[49] The Minister must be satisfied that gathering the intelligence is necessary for the proper performance of one of ASIS's statutory functions, and the person or class of persons is involved in one of a list of specified activities (such as acting for a foreign power, or other activities that pose a threat to Australia's security).[50] ISA 2001 s14 waives any liability for ASIS in respect of acts committed overseas that would be unlawful if done pursuant to a proper function of the agency. That waiver does not extend to activities inside Australia that ASIO could not carry out without a warrant, but it may well include interceptions overseas.

---

46 TIA 1979 s180F.

47 The Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2012, drafted by the Communications Access Co-ordinator.

48 TIA 1979 s186.

49 TIA 1979 s9.

50 ISA 2001 s9.

Oversight

27. Oversight of the interception process is provided in Australia by three mechanisms. Firstly, the Parliamentary Joint Committee on Intelligence and Security oversees the administration and expenditure of the Australian intelligence community, including ASIO. It is made up of members of both houses of Parliament nominated by the governing party, in consultation with all the parties in Parliament, although with a majority made up of the party currently in government. It reports to Parliament once a year, and will also review any amendments to include new agencies in the list of those which may authorise the disclosure of metadata.[51]

28. Secondly, the Inspector General of Intelligence and Security **[IGIS]** is established by the Inspector General of Intelligence and Security Act 1986 **[IGIS Act]**. It is a largely investigatory role, appointed for five years. He carries out broad-ranging investigations into the actions of the agencies at his own initiative or pursuant to a complaint or a request from the public or from ministers, including the Prime Minister.[52] He must seek the approval of the Prime Minister or a responsible Minister before investigating actions that took place outside of Australia.[53]

29. The IGIS is appointed by the Governor-General on the advice of the Prime Minister. The office is accountable to the Prime Minister but does not take directions from him. IGIS provides an annual report to the Prime Minister, who may redact that report before laying it before Parliament, although an unredacted version must be made available to the leader of the opposition.

30. As part of his role, IGIS also conducts regular inspections and investigations. Amongst those inspections are regular reviews of the documents that ASIO has relied on as providing the basis for its interception warrants.

31. Thirdly, the Commonwealth Ombudsman investigates the use of interception powers by law enforcement agencies, including through regular inspections of their records.[54] The office does not have jurisdiction over the intelligence agencies.[55] The Ombudsman must also inspect the records of enforcement agencies to determine their compliance with the new metadata regime.[56]

Canada

32. Canadian law provides a separate authorisation mechanism for the police and the security services to collect data.

Criminal law enforcement

33. Part VI of the Criminal Code, added pursuant to the Protection of Privacy Act 1974, provides for the grant of judicial warrants to intercept private communications. Private

51 TIS 1979 ss110A(11) and 176A(11).
52 IGIS Act s8.
53 IGIS Act s9AA.
54 Ombudsman Act 1976 s5.
55 Ombudsman Regulations 1977 sch. 1.
56 TIA 1979 s186B.

communications are defined as "*any oral communication or any telecommunication that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it.*"

34. In order to obtain an interception warrant, the police must make an application to a judge of a superior court of criminal jurisdiction that is signed by the Attorney General of the province in which it is made (or an agent specified for this purpose by the Government). It must be accompanied by an affidavit setting out (s185):

> "... (c) the facts relied on to justify the belief that an authorization should be given together with particulars of the offence;
>
> (d) the type of private communication proposed to be intercepted;
>
> (e) the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence, a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted and a general description of the manner of interception proposed to be used;
>
> (f) the number of instances, if any, on which an application has been made under this section in relation to the offence and a person named in the affidavit pursuant to paragraph (e) and on which the application was withdrawn or no authorization was given, the date on which each application was made and the name of the judge to whom each application was made;
>
> (g) the period for which the authorization is requested; and
>
> (h) whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."[57]

35. The application is made *ex parte* and is heard confidentially. However, targets of interceptions must be given notice of that fact they have been subject to surveillance, within 90 days of the authorisation having expired. A confidentiality extension may be granted up to three years after the investigation has come to a close (s196) in terrorism offence cases, where the judge is persuaded that it is in the "*interests of justice*". There are special provisions for obtaining an urgent authorisation from the judge (s188).

36. Stored communications, for example in cloud storage or on a personal computer, may also be accessed via a production order or search warrant. A search warrant may be granted by a judge who is satisfied that there are reasonable grounds to believe that there is "*anything on or in respect of which any offence"* has been or is suspected to

[57] Subsection (h) does not apply to some serious crimes and terrorism offences.

be committed, or evidence as to commission of an offence or the whereabouts of a person who is believed to have committed an offence.[58] A judge may also order a person, other than a person under investigation for an offence, to produce documents or prepare a document based on data already in existence and produce it.[59]

37. There is some confusion within Canadian law concerning whether emails that have already been sent should be governed by intercept or search warrants. In *R v Telus* (2013) SCC 16, the Supreme Court interpreted "*interception*" purposively, holding held that a warrant requiring a service provider to prospectively provide access to text messages was invalid: the police were seeking an "*interception*," as the service provider stored text messages on their servers as part of the communication and transmission process. Thus it is likely that the Royal Canadian Mounted Police should use their intercept powers, not those for search warrants, when seeking prospective access to email.

38. In late 2014, the Canadian Parliament passed the PCFOC 2014 that amended certain aspects of the Criminal Code. It provided for a clearer and more comprehensive framework for access to metadata by judicial warrant or court order, on a "*reasonable grounds to suspect*" standard (one that is lower than the more traditional reasonable grounds to believe threshold).[60]

Access for the Security Services

39. The CSIS are regulated by the CSIS Act 1984, which distinguishes between "*security intelligence*" and "*foreign intelligence."* The former relates to national security threats; the latter to the political or economic activities of foreign states. Save in relation to the s16 exception set out below, CSIS's role relates to the collection and analysis of security intelligence, and it is broadly the equivalent of MI5.

40. The CSIS Act 1984 s12 provides, where relevant:

> "The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada."

41. The s16 exception provides that the service may collect information or intelligence in relation to any foreign state as long as that information does not relate to a Canadian citizen, permanent resident or Canadian corporation and is done in Canada.

42. Warrant applications are made to a special bank of 14 specially selected and security cleared Federal Court judges, who meet up twice a year to ensure consistency. They largely hear warrant applications alone but may sit in larger numbers to hear an application and to hear submissions from CSIS on a topic of wider interest, although in

---

58 Section 487.1.

59 Section 487.12. A separate provision concerns provision of financial data of those suspected of Terrorist Financing or Money Laundering (487.13).

60 Criminal Code 417.014-018.

such cases the substantive decision is still taken by a single presiding judge. They are entitled to appoint an *amicus* advocate to make submissions in respect of the privacy issues raised by the application. I was told, in the course of my meeting with several judges of the Court, that they frequently appoint *amicus* counsel when novel warrants are sought that deploy new technology or propose new applications of old technology. The members of the Court were of the view that those counsel provided them with real assistance. I was told that warrant applicants can be made, heard and determined within 24 hours, and dealt with even faster in an emergency. The ordinary time lag is around 3 days.

43. The applicants are subject to a high duty of candour and may not omit relevant or important information. They will be criticised for failing to do so, as they were in *X(Re)* (2013) FC 1275, when Judge Mosley concluded they had deliberately suppressed their intention to monitor Canadian terror suspects outside of Canada (via cooperation with other Five Eyes members).[61]

44. In addition to the judges (who sit on rotation), the Designated Proceedings Registry employs eight full time staff and one full time senior counsel. The Registry's annual budget (excluding infrastructure and some IT costs) was $826,000 last year (*circa* £430,000). During 2013-14 the Federal Court dealt with 85 new warrant applications and 178 renewal applications.

45. A warrant must be supported by an affidavit, which I am told are ordinarily between 35 and 200 pages long. They set out (amongst other things):

    (a) Why the applicant believes "*on reasonable grounds*" that the warrant is necessary for the Service to carry out its role;

    (b) Other procedures have been tried and failed or are unlikely to succeed;

    (c) The type of communication to be intercepted or information, records, documents or things to be obtained;

    (d) The identity of the person whose communication is proposed to be intercepted (if known); and

    (e) Any previous applications in respect of that person.

46. A warrant may not be issued for longer than 60 days, where it is issued to enable the Service to investigate "*threats to the security of Canada*", or one year in any other case.

47. Thus, this warrant process involves a two-stage review process: by the Minister and also by the court. The judicial element was introduced following a series of reports into abuses carried out by the Canadian police Security Services in the 1970s.

48. In 2008 in *Re CSIS*, the Federal Court held that the CSIS had no power to carry out activities beyond Canadian borders because the CSIS Act is not extraterritorial in scope, or at least did not authorize overseas conduct that was not in compliance with

[61] The judgment was upheld by the Court of Appeal (*Re(X)* 2014 FCA 249)

foreign laws (and thus violated foreign sovereignty). As a practical result, the power to covertly collect information (pursuant to a s21 warrant) relating to foreign affairs is restricted to the right to take steps within Canada itself. The effects of that decision were reversed by PCFOC 2014 which provided that CSIS may perform its duties and functions outside of Canada. It expressly authorises a judge to issue a warrant for overseas investigations, even if those investigations may be violation of foreign or other laws.

49. Sections 34 and onwards of the Act establish the SIRC, composed of members of the Canadian Privy Council. Those who sit on SIRC are not ordinarily members of the Senate or House of Commons. The Governor in Council (in practice, the Canadian federal cabinet) appoints the members of the Committee in consultation with the Prime Minister, Leader of the Opposition and the leader of each party with at least 12 Members of the House of Commons. The individuals appointed play an important but comparatively limited role in the operations of SIRC. They retain other obligations and ordinarily only meet a small number of times per year. The day-to-day operations of SIRC are carried out by its full time staff of 18 individuals.

50. The Committee is required to review the Service in general, although the statute does not specify that it should review the warrantry process. However, in practice SIRC reviews a random sample of all warrant applications in any given year (around 5%). That review involves an examination of the underlying documents that led to the warrant application, that were not provided to the court in the application. Their reports are provided to the Minister and the Director of the Service. SIRC also prepares an annual report recounting its operations and summarising its findings and recommendations.

51. Any individual may complain of the Service's activities to the Committee, which is entitled to investigate and make recommendations. .[62] SIRC has no powers to enforce its holdings. It is competent only to make recommendations.

52. The National Defence Act 1985 **[NDA 1985]** recognised the existence of what is now the CSE, a signals intelligence agency and the Canadian equivalent of GCHQ. NDA 1985 defined CSE's mandate as:

> "(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
>
> (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
>
> (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."[63]

62 Section 37.
63 273.64(1).

53. In conducting its mandate (a) and (b) functions, CSE may not direct its activities at Canadians or any person in Canada and their activities are subject to measures to protect the privacy of Canadians in the use and retention of intercepted material. When CSE performs its mandate (c) function providing assistance to federal law enforcement and security services, it is sheltered by those bodies' lawful authority (e.g., a Part VI authorization or CSIS Act warrant).

54. When CSE collects foreign intelligence, this is generally an internal decision with no legislated oversight requirements. However, in the course of collecting foreign intelligence through signals intelligence operations, CSE may sweep up incidental "*private communications*" – that is communications involving Canadians or persons in Canada. To prevent this from being a violation of the Criminal Code's Part VI prohibition on unlawful intercepts, the NDA 1985 puts in place a special authorization regime, involving the Minister of National Defence. Unlike CSIS, CSE may be authorised by the Minister to obtain foreign intelligence that may involve private communications without reference to the courts. The Minister must be satisfied that the interception will be directed at foreign entities outside Canada, the information could not be obtained by other means, the value of the material justifies the interception and that satisfactory measures are in place to protect the privacy of Canadians and to ensure that the material will only be used or retained if they are essential to international affairs, defence or security. These broad powers stand in some contrast to the focused and specific warrantry process for CSIS.

55. While CSE has historically adopted the position that a ministerial authorisation was not required before it obtained access to metadata, following *Telus* and *Spencer*, and the changes introduced by PCFOC 2014, that position is no longer arguable.

56. NDA 1985 requires the appointment of a supernumerary (retired) judge as a Commissioner of CSE to review its activities and investigate any complaints (section 273.63). The current Commissioner is supported by 11 staff members. His operation costs a little under $2 million Canadian dollars per year.[64] Among other things, the Commissioner reviews any new ministerial authorisations relating to private communication on a provisional basis and then addresses them in more detail in his annual review. His staff are also given access to the data analysis engineers within CSE and may confirm the processes and uses that it is subjected to.

57. The Commissioner's reports have been an important source of information concerning what mechanisms are employed by CSE and also how it interprets its obligations. In particular, the 2012 Commissioner's report disclosed CSE's policy concerning the private communications of Canadian citizens that are the 'bycatch' of a foreign intelligence collection:

    (a) They must be destroyed, save where the material is foreign intelligence or material essential to protect the lives or safety of individuals of any nationality, or where it contains information on serious criminal activity relating to the

64 http://www.ocsec-bccst.gc.ca/ann-rpt/2013-2014/ann-rpt_e.pdf p. 13.

security of Canada or is essential to identify, isolate or prevent harm to the Canadian Government's computer systems.

(b) At the expiry of an authorisation, CSE must report to the Ministry of National Defence explaining what Canadian communications were retained and on what basis.[65]

(c) When CSE shares information with its global partners, the names of any Canadian are redacted and only reinstated at the specific request of a partner country and after CSE has satisfied itself that the requesting government department has proper authority and justification to make the request.[66]

New Zealand

The Security and Intelligence Service

58. NZSIS is New Zealand's equivalent of MI5, and is governed by the New Zealand Security Intelligence Service Act 1969 **[SISA 1979]**.

59. Like Canada, America (and to some extent Australia), New Zealand provides for judicial oversight of the warrant process at the point of authorisation. However, unlike those countries, that oversight is provided by a retired High Court Judge, the Commissioner of Security Warrants. The Commissioner is a creature of statute, created in 1999.[67]

60. Domestic warrant applications are jointly signed off by both the Minister and the Commissioner. The applicant must provide sworn witness evidence that the interception is necessary for the detection of activities prejudicial to security or for the purpose of gathering foreign intelligence information essential to security. They must also provide evidence that any communication sought to be intercepted is not privileged and that the information is not be obtained by any other means.[68]

61. Foreign intelligence warrants operate differently. Firstly, the Commissioner is not involved in their authorisation. Secondly, as well as satisfying the conditions above, NZSIS must demonstrate that that there are reasonable grounds for believing that no New Zealand citizen or permanent resident is to be identified by the proposed warrant as a person who is to be subject to the warrant and that any place to be specified in the proposed warrant is occupied by a foreign organisation or a foreign person.

62. Whether internal or foreign, intelligence warrants must specify the type of communication to be intercepted, the identity of the persons (if known) whose communications are sought to be intercepted and (if not known) the place or facility in respect of which communications may be intercepted.[69] Given the restrictive nature of those requirements, it is unlikely that NZSIS has any power to carry out bulk interception.

---

65 *Ibid.,* p. 14-15.
66 *Ibid*., p. 27.
67 SISA 1979 s5A.
68 SISA 1979 s4A.
69 SISA 1979 s4B.

63. SISA 1979 also contains provisions relating to destruction of irrelevant data.

The Government Communications Security Bureau

64. The GCSB was originally a branch of the Ministry of Defence. It bears some resemblance to GCHQ in the United Kingdom. The Director of GCSB may apply in writing to the Minister for an interception warrant authorising the interception of:[70]

(a) Communications made or received by one or more persons or classes of persons specified in the authorisation or made and received in one or more places or classes of places specified in the authorisation;

(b) Communications sent from, or being sent to an overseas country; or

(c) The accessing of one of more specified information infrastructures or classes of information infrastructures that the Bureau cannot otherwise lawfully access.

65. As under SISA 1979, any application for a warrant or access authorisation must be made jointly to the Minister and the Commissioner of Security Warrants, if anything done under the warrant is for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident.[71] If the warrant or authorisation is not sought for the purpose of intercepting the private communications of a person who is a New Zealand citizen or permanent resident, only the Minister needs to agree it.[72]

66. The Minister and Commissioner may grant the interception warrant if satisfied that it is for the purpose of performing the Bureau's functions; the outcome justifies the interception; it cannot be achieved by other means; there are satisfactory arrangements to ensure that nothing will be done in reliance on the warrant that goes beyond what is necessary; and anything done will be reasonable, having regard to the purposes of the warrant itself.[73] As with SISA 1979, no warrant may be issued for the purpose of intercepting privileged communications.

67. Interception without a warrant may take place in certain narrow circumstances, when the interception does not involve physically connecting an interception device to any information infrastructure or installing an interception device in a place; any access to information infrastructure is "*limited to access to one or more communication links between computers or to remote terminals*" and it is carried out in pursuance of either advising or cooperating with public authorities in terms of protecting communications and infrastructures, or regarding foreign intelligence.[74]

Police Surveillance

68. The Search and Surveillance Act 2012 **[SSA 2012]** sets out a comprehensive regime governing all species of warrant, including warrants for entry, warrants to set up road blocks and interception under a warrant. A warrant is necessary if an enforcement

70 GCSB Act s15A(1).
71 GCSB Act s15B.
72 GCSB Act s14.
73 GCSB Act ss15A(2).
74 GCSB Act s16.

officer wishes to use an interception device to intercept a private communication (as well as various other forms of surveillance).[75]

69. An application for a surveillance device warrant (which includes a warrant to use an interception device) must be made in writing and set out in "*reasonable detail*": the name of the applicant, the provision that authorises the application, the grounds on which it is made, the suspected offence in relation to which authorisation is sought, the type of device, the name address or other description of the person, place, vehicle or thing that is the object of surveillance, what material it is hoped to obtain and the period for which the warrant is sought.[76] If the person, place, thing or vehicle cannot be identified, the application must at least define the parameters of and objectives of the operation. An application may only be made by a constable or an enforcement officer that has been approved by an Order in Council.[77]

70. Other law enforcement bodies than the police may only undertake interception if they have been designated by an Order in Council made by the Governor-General.[78]

71. The application should be made to a Judge, who must be satisfied that there are reasonable grounds to suspect that an offence has been or is being or will be committed and that that offence falls within a list of sufficiently serious crimes, set out in the Schedule to the Act.[79] The Judge must also be convinced that the interception will obtain evidential material.

72. There are mechanisms for obtaining a warrant in an emergency, where there is insufficient time to secure access to a Judge.[80]

Access to Metadata

73. The law concerning access to communications data, or metadata, was unclear until recently. In 2013 it was disclosed that GCSB had taken the view that metadata was not a communication and so could be obtained without a warrant (or indeed any other formal authorisation mechanism).[81] TICSA 2013 has set the position out on a statutory footing. It defines "*call associated data*" as information generated as a result of making a telecommunication that includes the number from which it originates, the number to which it was sent, if it is diverted then the number at which it was received, the time at which it was sent, its duration, if it was from a mobile phone the point at which it first entered the network.[82]

74. Public telecommunications service providers are required to be capable of obtaining call associated data (other than telecommunications that are not authorised to be intercepted under the warrant or lawful authority).[83] That information should be

75 SSA 2012 s46.
76 SSA 2012 s49(1).
77 SSA 2012 s49(5).
78 SSA 2012 s50(1).
79 SSA 2012 s51(1).
80 SSA s48.
81 Kitteridge Report on GCSB Compliance, available online at: http://www.gcsb.govt.nz/assets/GCSB-Compliance-Review/Review-of-Compliance.pdf para 23.
82 TICSA 2013 s3.
83 TICSA 2013 s10.

provided, on presentation of a proper warrant, to GCSB, SIS or the New Zealand Police.

75. A fresh round of Snowden disclosures in 2014 suggested that GCSB had developed a mass metadata collection program known as SPEARGUN. The basic premise of the alleged program was to insert metadata probes into the Southern Cross Cable, which carries much of New Zealand's telecommunications. Prime Minister John Key admitted that the project had been initiated but denied that it had become operational because he had vetoed it. The controversy arose, in part, as the broad powers under GCSB Act ss15 and 15A were not in place during 2012, when the project was allegedly begun.[84]

Oversight

76. The New Zealand security services are overseen via a number of statutory mechanisms. First, the Intelligence and Security Committee is a Parliamentary body, established in statute, which is made up of five persons including the Prime Minister, Leader of the Opposition and 3 other Members of Parliament.[85] It examines the policies and administration of the Security Intelligence Service and GCSB and consider other questions with intelligence or security implications that are referred to it by the Prime Minister.

77. Second, the Inspector-General of Intelligence and Security, is an individual appointed by the Governor General, on the recommendation of the Prime Minister.[86] The Inspector-General enquires into the Services' compliance with its legal obligations and complaints about its activities. They are specifically required to review, at least once every 12 months, the compliance with the governing legislation in relation to the issue and execution of warrants and authorisations.[87] The Inspector-General reports annually to the Prime Minister and a redacted version of that report is laid before Parliament.

78. Third, as set out above, the Commissioner of Security Warrants is engaged in agreeing to any warrant granted to the security service that will collect the communications of New Zealand citizens or residents.

The United States of America

79. The US law concerning investigatory powers is divided between two separate statutory frameworks. The WA 1968, the Stored Communications Act **[SCA]** and Pen Register Act **[PRA]** govern the use of investigatory powers in conventional criminal law enforcement.[88] A separate regime, the Foreign Intelligence Services Act 1978 **[FISA 1978]**, governs the collection and analysis of foreign intelligence. Both frameworks have been extensively amended since their introduction.

---

84 https://firstlook.org/theintercept/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/
85 Intelligence and Security Committee Act 1996.
86 Inspector-General of Intelligence and Security Act 1996 **[IGISA]** s. 5.
87 IGISA s11(d).
88 US Civil Code Title 18 Chapter 119. SCA and PRA were introduced under the Electronic Communications Privacy Act 1986, which substantially amended the WA 1968.

Criminal law enforcement

80. The WA 1968 governs interception of wireless, oral and electronic communications within the United States. It defines intercept as "*the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.*"[89] Access to information that is not in the course of transmission, is governed by the SCA.[90]

81. All interceptions under the WA 1968 must be authorised by a court and are subject to careful review. US Code s2516 of Title 18 sets out the basis on which law enforcement staff, inside the United States, may be given authority to intercept communications. Various senior officials within federal law enforcement agencies (such as the FBI or the Attorney General's office) may authorise an application to a Federal Judge of competent jurisdiction for an interception warrant.[91] The application must be in writing, on oath and set out the facts and circumstances in some detail. I was told by law enforcement agencies that these applications are frequently substantial documents. An application may only be made in order to provide evidence (from the wiretap) that will be relevant to certain serious federal felonies. If the application is for an extension, it must set out the results obtained thus far or a reasonable explanation for the failure to obtain results under the previous warrant.[92]

82. The court must be satisfied that there is "*probable cause for belief*" that:[93]

    (a) An offence has been or is about to be committed;

    (b) Communications confirming the commission of the offence will be obtained;

    (c) Normal investigative procedures have been tried and failed or are unlikely to succeed;

    (d) The communications method is or will be used in connection with the commission of the offense.

83. The third of those criteria is not required for other types of investigatory warrant, such as a search warrant. As a result, interception warrants are sometimes referred to as "*super warrants*". The warrant shall not continue for longer than is necessary and may not be issued for more than 30 days.[94] In an emergency situation an interception may begin without an application to the court, if an application is made within 48 hours.[95]

84. The ordinary position under the WA 1968 is that an inventory of the fact of interception, dates and whether anything was intercepted is provided to the persons named in the order within 90 days of termination unless the authority can show "*good cause*" to

89 18 U.S.C § 2510(4).
90 As is the case in the United Kingdom, the precise boundary between data that is "*in the course of transmission*" and communications data is a complex area of some uncertainty.
91 18 U.S.C. § 2516 (1).
92 18 U.S.C. § 2518 (1)(f).
93 *Ibid*. at (3).
94 *Ibid*. at (5).
95 *Ibid*. at (7).

withhold that information at an *ex parte* hearing.[96] I was told, during my trip to the United States, that disclosure to the subject ordinarily occurs in the context of a criminal procedure. Those individuals who receive notification that they have had their communications intercepted but are not party to any criminal trial, rarely bring proceedings seeking damages. Such damages are capped in any event.

85. US Code Chapter 21 of Title 18, commonly referred to as the SCA, provides access for law enforcement to both contents and metadata that are stored on a Remote Computing Service. This provides computer storage or processing services to the public by means of an electronic communications system,[97] such as cloud storage. Access to the content of stored communications, without notice, is granted on the basis of a search warrant.[98] Access to stored material that does not include the content of communications may be granted on a similar basis.[99]

86. However, and importantly, a specified subset of non-content may be accessed by administrative subpoena without the scrutiny or authorisation of a court. Those data are: name, address, call records, length of service, types of service used, number used including temporarily assigned IP address, means and source of payment.[100] As a result, much of the most important metadata may be obtained without the permission of a court.

87. Furthermore, the SCA provides for access to metadata records, without judicial authorisation, where the Director of the FBI (or his designee) certifies that they are relevant to an authorised investigation to protect against international terrorism or clandestine intelligence activities. Those requests are known as "*National Security Letters*". The Director of the FBI may request, and a telecoms provider is required to provide, name, address, length of service and local and long distance toll billing records on that basis.[101]

88. An important distinction between US and UK law (as it currently stands) is that there is no requirement for service providers in the United States to store data beyond their own business needs. I was informed during my trip to the US that it was highly unlikely that Congress would consider legislation requiring service providers to retain or create data that they did not themselves need for business purposes (such as billing). However, telecommunications providers are required to retain data that they already produce and create such as: name, address, telephone number of the caller, telephone number called, date, time and length of a call.[102] If law enforcement agencies want access to material beyond that, or want access to other metadata, they are empowered to request that material is preserved, pending an application for access to that data.[103]

---

96 *Ibid*. at (8)(d).

97 18 U.S.C. § 2711(2).

98 If the data owner is put on notice, it may also be accessed via a court order, administrative subpoena or grand jury or trial subpoena 18 U.S.C. § 2703.

99 Search warrant, telemarketing fraud request or court order. It is important to note that for non-content subscriber records, no notice has to be given to the subscriber.

100 18 U.S.C. § 2703 (2).

101 18 U.S.C. § 2709 (b).

102 17 C.F.R. § 42.6.

103 E.g. 18 U.S.C. § 2704.

89. Finally PRA grants both federal and state law enforcement the right to make records of outgoing numbers from (pen register) and incoming calls (trap and trace) to a particular phone number pursuant to a court order.[104] The definition of a "*pen register*" was widened by the USA PATRIOT Act in 2001. It now includes a device which records "*signalling information"* that can record access to the internet and other network analysis devices.[105] The procedure for obtaining a court order is less onerous than the procedure for obtaining a warrant, both in terms of the standard of proof to be met and the level of detail that is ordinarily provided.[106] Court orders under the PRA last for up to 60 days. They do not provide a basis for gaining access to the contents of communications.

Gathering of foreign intelligence

90. FISA 1978 (as amended) authorises the electronic surveillance of foreign powers overseas - including groups engaged in international terrorism - and agents of foreign powers. Much of the material collected under FISA 1978 is gathered overseas or concerns the activities of non-US citizens in the mainland United States. However, a US person may also be an agent of a foreign power,[107] to the extent that they knowingly gather intelligence for a foreign power or engage in sabotage or terrorism on behalf of a foreign power.

91. FISA 1978 authorises broadly three kinds of data collection. First the traditional FISA 1978 process requires a Federal officer, with the approval of the Attorney General, to apply to the FISC, a bespoke federal court made up of eleven district court judges set up following reports of abuse by the intelligence agencies in the United States, for an interception warrant. Those eleven judges sit part time, at the court for one week stints on duty, where they read or hear warrant applications under FISA 1978. The Court has 10 full time staff members: five counsel to the Court and five administrative staff.[108]

92. The majority of applications are dealt with on the papers though I was informed that around 10% are dealt with following an oral hearing.[109] The judges can and do request that the individual who swore an affidavit in support of the application appears before them so that they can be asked questions by the judge. No special advocate can appear to make submissions in defence of the privacy interests in issue. The court has recently accepted an amicus brief from the Centre for National Security Studies on the question of bulk metadata production.[110] However, I am not aware of amicus counsel being instructed to make submissions in specific cases. Historically very few judgements of the FISC have been published. However, there has been a trend towards publication in recent years. A telecommunications provider, that is ordered to provide access to material, or a government body that has applied for a warrant may

104 18 U.S.C. § 3121.
105 18 U.S.C. § 3127 (3).
106 18 U.S.C. § 3122.
107 Defined as a citizen of the US, an alien with lawful permanent residence or a US corporation or unincorporated association.
108 The court does not publish details of its costs but the District Court Judges are not paid any additional salary for their FISC work.
109 In the calendar year 2013, the FISC received 1,655 applications under s 702, 178 applications for "*tangible things*" under s215 and the FBI applied for 14,219 National Security Letters.
110 http://www.fisc.uscourts.gov/sites/default/files/Misc%2014-01%20Order-1.pdf.

appeal a decision of the FISC to the United States Foreign Intelligence Surveillance Court of Review. In practice, such appeals are rare.

93. An application for a FISA 1978 warrant must specify the identity (if known) or a description of the specific target of the electronic surveillance. It must set out the facts and circumstances to support the belief that the target is a foreign power or agent of a foreign power and that the targeted facilities will be used by them.[111] The application must also set out the minimisation procedures in place to ensure that the correspondence of United States persons is not acquired, retained or distributed.[112]

94. The judge of the FISC must be satisfied that there is probable cause to believe that the elements above are satisfied (including that the target is a foreign power or agent of a foreign power). An order may be granted for up to 90 days.[113] FISA 1978 orders may be granted that authorise the interception of the communications of US citizens, to the extent that the FISC judge is satisfied that there is probable cause to find that that individual is an agent of a foreign power.

95. The second, more controversial, aspect of FISA 1978 arises out of a series of amendments to the Act introduced in 2008 (the FISA Amendment Act 2008 Section 702 allows the targeting of individuals "*reasonably believed to be located outside the United States to acquire foreign intelligence information*" without the same degree of judicial scrutiny.[114] Under s702, the Attorney General and the Director of National Intelligence may jointly authorise that targeting for a period of up to one year. Acquisition of data via this route may not intentionally target:

(a) Any person known to be located in the United States;

(b) A person outside of the United States in order to target a person reasonably believed to be in the United States;

(c) A United States person reasonably believed to be outside the United States; or

(d) Any communication as to which the sender and recipients are all known to be inside the United States.

96. The basic mechanics of s702 are:

(a) The Attorney General and Director of National Intelligence draw up a certificate identifying categories of foreign intelligence that they wish to collect (for example email addresses of suspected terrorists overseas). Those certifications do not contain the level of specificity as to the individual targeted that is required under a normal FISA 1978 order;

(b) The certification must set out the targeting procedures that will be used. They must be "*reasonably designed"* to ensure that the material acquired is "*limited to targeting persons reasonably believed to be located outside the United*

111 50 U.S.C. § 1804 (a).
112 See: 50 U.S.C. § 1801.
113 50 U.S.C. § 1805.
114 50 U.S.C § 1881a.

States." The certification must also attest that the Attorney General has adopted Guidelines to ensure compliance with the s702 framework.

(c) A judge of the FISC reviews the minimisation and targeting provisions of those certifications before they are implemented. They must be satisfied that the targeting procedures are "*reasonably designed*" to meet the objectives set out above.[115] The presiding judge writes an opinion setting out why he or she considers that the procedures meet that standard and also why they comply with the First Amendment right to free speech.

(d) However, the judge does not have to approve the targeting decisions: they do not have to satisfy themselves that the target (or targets) are a foreign power or agents of a foreign power.[116]

(e) The NSA have published a fact sheet on their minimisation procedures, which provides that inadvertently acquired communication of or concerning a US person must be promptly destroyed if it is neither relevant to the authorised purpose or evidence of a crime.[117]

97. The Inspector General assesses compliance with the procedural requirements and reports on them on an annual basis to Congress. The Attorney General also submits a report to Congress each year setting out the number of applications and extensions of s702 surveillance certificates and the number of those orders or extensions granted, modified or denied.[118] He also submits a semi-annual assessment to three Congressional select committees concerning all electronic surveillance under s702.[119]

98. Section 702 provided the basis for the US Government to carry out its PRISM and Upstream collection programs (described more fully at Annex 7 to this Report).

99. A third, and equally controversial, aspect of FISA 1978 is Subchapter IV: Access to Certain Business Records for Foreign Intelligence Purposes (known as s215). It provides that the Director of the FBI, or a designee, may make an application for an order requiring the production of any "*tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities*."[120]

100. An application under s215 should be made to the FISC and include a statement of facts showing that there are reasonable grounds to believe that the things sought are relevant to an authorised investigation.[121] If the court is satisfied that that is the case, it will issue an order that describes the tangible things that must be provided "*with sufficient particularity to permit them to be fairly identified*."

115 50 U.S.C. § 1881a (i) (2)(B)(i)
116 50 USC § 1881a (g).
117 https://www.fas.org/irp/news/2013/06/nsa-sect702.pdf.
118 50 U.S.C. § 1807.
119 50 U.S.C. § 1808.
120 50 U.S.C. § 1861(1).
121 *Ibid*. 1861(1) (b).

101. Section 215 has become controversial in the light of the disclosures in the Snowden Documents, when it became clear that the FBI had applied, on behalf of the NSA, for orders authorising the collection of nearly all call information generated by certain telephone companies in the USA. The NSA had then queried the database of information that resulted by enquiring for all calls to or from telephone numbers in respect of which there was a "*Reasonable Articulable Suspicion*" that it was associated with terrorism (the seed number). The NSA then operated a system known as contact chaining whereby all persons in contact with the seed number - the first hop - all numbers directly in contact with the first hop numbers (the second hop) and all numbers in contact with those second hop numbers as well (the third hop) could be accessed and stored.[122] The judges of the FISC had authorised that program pursuant to a series of 90 day orders.

102. Finally, EO 12333 provides an extra-statutory basis for the intelligence services to carry out interception of communications. It was first issued in 1981 and has been amended on three occasions since. Part 1 of EO 12333 sets out the various roles of the intelligence bodies in the United States. Part 2 includes a broad power to collect information. Comparatively little is known about the use of those powers. If it is relied upon as a basis for carrying out interception, the intelligence agencies may do so without judicial authorisation.

Oversight

103. The intelligence services in the United States are subject to multiple forms of oversight. In 2007 Congress established a Privacy and Civil Liberties Oversight Board to review and oversee civil liberties in the context of national security. The Board has published two report. Its first, in January 2014 concerned the "*section 215 program*" and held that it did not comply with the statute itself. In particular, the Board held that the program had been authorised by reference to counter-terrorism investigations in general, and not a specific authorised investigation (as required). They also expressed their serious reservations about whether or not it complied with the Constitution.[123] A second report in July 2014, concerning s702 concluded that certain historical programs "*push the program close to the line of constitutional reasonableness."*[124] However, they concluded that the program was, in broad terms, lawful. Both Houses of Congress also provide legislative oversight in the form of a permanent select committee on intelligence.

104. A separate President's Intelligence Oversight Board reports directly to the President on potential violations of the law committed by the Agencies. Many of the Agencies themselves also contain an Office of Inspector General, with a remit to review compliance internally.[125]

---

122 Following a change in 2014 the FISC now has to approve RAS determinations before contact chaining may be carried out.

123 http://www.fas.org/irp/offdocs/pclob-215.pdf. That was a view shared by the President's Review Group on Intelligence and Communications Technologies, p. 85. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

124 http://www.pclob.gov/library.html page 9.

125 17th Report of Session 2013-14, HC231 (May 2014), p. 92.