PRIVACY INTERNATIONAL

62 Britton St
London, EC1M 5UY
Great Britain
T +44 (0) 7788 286 389
info@privacy.org
www.privacyinternational.org

2 December 2013

Vivienne Thom
Inspector-General of Intelligence and Security
PO Box 6181
KINGSTON ACT 2604
Australia
By email: info@igis.gov.au

Dear Ms Thom,

Re: Complaint against the Australian Signals Directorate

1. We wish to submit a complaint against the Australian Signals Directorate on behalf of the author, an Australian citizen, under s 10(1) of the *Inspector-General of Intelligence and Security Act 1986* (hereafter "the IGIS Act"). The basis for our complaint is set out below.

The relevant legislation

2. We submit that the Australian Signals Directorate (hereafter "ASD") has acted in a manner that violates the laws of the Commonwealth and is contrary to guidelines given to the agency by the responsible Minister, warranting an investigation by your office under sections 8(2)(a)(i) and (ii). In the alternative, we submit that the ASD has acted with impropriety, warranting an investigation under section 8(2)(a)(iii).

3. Section 7 of the *Intelligence Services Act 2001* (hereafter the ISA) prescribes the functions of the ASD:
    a. to obtain intelligence about the capabilities, intentions or activities of people or organisations outside Australia in the form of electromagnetic energy, whether guided or unguided or both, or in the form of electrical, magnetic or acoustic energy, for the purposes of meeting the requirements of the Government, and in particular the requirements of the Defence Force, for such intelligence; and
    b. to communicate, in accordance with the Government's requirements, such intelligence; and
    c. to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; and

d. to provide assistance to the Defence Force in support of military operations and to cooperate with the Defence Force on intelligence matters; and
e. to provide assistance to Commonwealth and State authorities in relation to:
   (i) cryptography, and communication and computer technologies; and
   (ii) other specialised technologies acquired in connection with the performance of its other functions; and
   (iii) the performance by those authorities of search and rescue functions; and
f. to co-operate with and assist bodies referred to in section 13A in accordance with that section.

4. Section 11 prescribes the functions of the agencies to only those performed "in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being and only to the extent that those matters are affected by the capabilities, intentions or activities of people or organisations outside Australia."

5. Pursuant to section 11(2AA), intelligence agencies may communicate incidentally obtained intelligence to appropriate Commonwealth or State authorities or to authorities of other countries approved under section 13(1)(c) if the intelligence relates to the involvement, or likely involvement, by a person in one or more of the following activities:

   a. activities that present a significant risk to a person's safety;
   b. acting for, or on behalf of, a foreign power;
   c. activities that are a threat to security;
   d. activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
   e. committing a serious crime.

6. Section 13(1)(c) permits the agency to cooperate with "authorities of other countries approved by the Minister as being capable of assisting the agency in the performance of its functions."

7. Section 15 of the ISA is entitled *Rules to protect privacy of Australians* and details the requirement that the responsible Minister in relation to the relevant agency must make written rules regulating the communications and retention by the relevant agency of intelligence information concerning Australian persons. Sub-section 5 of that provision stipulates that "[t]he agencies must not communicate intelligence information concerning Australian persons, except in accordance with the rules."

8. The ASD's Rules to Protect the Privacy of Australians were issued on 2 October 2012, and include the following pertinent provisions:

- Where DSD[1] does retain intelligence information concerning an Australian person, DSD is to ensure that "access to that information is only to be provided to persons who require such access for the proper performance of a DSD function" (Rule 2.2(b)).
- DSD may communicate intelligence information concerning Australian persons only where it is necessary to do so for the proper performance of DSD's functions or where such communication is authorised or required by or under another Act (Rule 3.1)).
- In addition, the following specific rules apply. Intelligence information concerning an Australian person may be communicated where "deletion of that part of the information concerning the Australian person would significantly diminish the utility of the information for the purposes of (i) maintaining Australia's national security; (ii) maintaining Australia's national economic well-being; (iii) promoting Australia's foreign relations; (iv) preventing or investigating the commission of a serious crime; (v) responding to an apparent threat to the safety of a person" (Rule 3.2(c)).
- In addition, intelligence information concerning an Australian person may be communicated where the information concerns a person "who is, or was at the time the information was collected, the subject of an authorization given by the Minister under section 9 of the Act" (Rule 3.2(d)).
- DSD may communicate intelligence information concerning an Australian person, that was not deliberately collected, to an authority with which DSD is permitted to cooperate, provided the Minister is satisfied that there are satisfactory arrangements in place to ensure that the authority will abide by the DSD privacy rules (Rule 4).

9. Where an activity, or a series of activities, produces intelligence on an Australian person, or will have a direct effect on an Australian person, section 8 of the Act requires the responsible Minister in relation to the relevant service to issue a written direction to the relevant agency head requiring the agency to obtain an authorization under section 9. Before a Minister gives an authorization under section 9 to enable intelligence collection vis a vis an Australian person the Minister must be satisfied that (s9(1))
    a. any activities which may be done in reliance on the authorisation will be necessary for the proper performance of a function of the agency concerned; and
    b. there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the agency; and
    c. there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out.

[1] DSD was renamed the Australian Signals Directorate in May 2013 "to more accurately reflect its national role".

10. Section 9(1A) also requires the Minister to be satisfied that the Australian person is involved in one of a number of activities, i.e.
    i. activities that present a significant risk to a person's safety;
    ii. acting for, or on behalf of, a foreign power;
    iii. activities that are, or are likely to be, a threat to security;
    iv. activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);
    v. activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law;
    vi. committing a serious crime by moving money, goods or people;
    vii. committing a serious crime by using or transferring intellectual property;
    viii. committing a serious crime by transmitting data or signals by means of guided and/or unguided electromagnetic energy.

11. If the Australian person is, or is likely to be, involved in an activity or activities that are, or are likely to be, a threat to security, the Minister must obtain the agreement of the Minister responsible for administering the *Australian Security Intelligence Organisation Act 1979* (s9(1A)(b)).

Acts or practices undertaken by the ASD in contravention of the ISA

12. Beginning in 1946, an alliance of five countries (the US, the UK, Australia, Canada and New Zealand) developed a series of bilateral agreements over more than a decade that became known as the UKUSA agreement, establishing the Five Eyes alliance for the purpose of sharing intelligence, but primarily signals intelligence (hereafter "SIGINT"). The original agreement mandated secrecy, stating "it will be contrary to this agreement to reveal its existence to any third party unless otherwise agreed," resulting in modern day references to the existence of the agreement by the intelligence agencies remaining limited. The existence of the agreement was not acknowledged publicly until March 1999, when the Australian government confirmed that the Defence Signals Directorate (now the ASD) "does co-operate with counterpart signals intelligence organisations overseas under the UKUSA relationship."[2]

13. The extent of the original arrangement is broad and includes the
    a. collection of traffic;
    b. acquisition of communications documents and equipment;
    c. traffic analysis;
    d. cryptanalysis;

[2] The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition, October 1999, page 1, available at:
http://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf

e. decryption and translation; and
f. acquisition of information regarding communications organizations, procedures, practices and equipment.

14. A draft of the original UKUSA agreement, declassified in 2010, explains that the exchange of the above-listed information

> "will be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon."

15. Indeed, in addition to facilitating collaboration, the agreement suggests that all intercepted material would be shared between Five Eyes States by default. The text stipulates that "all raw traffic shall continue to be exchanged except in cases where one or the other party agrees to forgo its copy." The level of co-operation under the UKUSA agreement is so complete that "the national product is often indistinguishable."[3] This has resulted in former intelligence officials explaining that the close-knit cooperation that exists under the UKUSA agreement means "that SIGINT customers in both capitals seldom know which country generated either the access or the product itself."[4] Another former British spy has said that "[c]ooperation between the two countries, particularly, in SIGINT, is so close that it becomes very difficult to know who is doing what [...] it's just organizational mess."[5]

16. Activities undertaken by the Five Eyes countries include, inter alia, interception of fibre optic cables, direct access to data held by corporate entities, computer network exploitation operations (hacking), infiltration of smartphones, collection of address books, and direct surveillance of foreign targets, foreign embassies and diplomats. It is believed that much of the intelligence collected under the Five Eyes arrangement can be accessed by any of the Five Eyes partners at any time. A core program that provides this capability is known as XKEYSCORE, which has been described by internal NSA presentations as an "analytic framework" which enables a single search to query a "3 day rolling buffer" of "all unfiltered data" stored at 150 global sites (including four in Australia) on 700 database servers.[6]

17. The ASD is a key member of the Five Eyes alliance and is heavily integrated with the NSA and GCHQ. A large amount of intelligence is collected and

---

[3] Robert Aldrich (2006) paper 'Transatlantic Intelligence and security co-operation', available at: http://www2.warwick.ac.uk/fac/soc/pais/people/aldrich/publications/inta80_4_08_aldrich.pdfIntelligence'

[4] S. Lander, 'International intelligence cooperation: an inside perspective', in Cambridge Review of International Affairs, 2007, vol. 17, n°3, p.487.

[5] Britain's GCHQ 'the brains,' America's NSA 'the money' behind spy alliance, Japan Times, 18 November 2013, accessible at: http://www.japantimes.co.jp/news/2013/11/18/world/britains-gchq-the-brains-americas-nsa-the-money-behind-spy-alliance/#.UozmbMvTnqB

[6] Snowden reveals Australia's links to US spy web, The Age, 8 July 2013, accessible at http://www.theage.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html

shared fluidly amongst all agencies in the alliance. Evidence of ASD's practical involvement includes activities such as:

a. Contributing intelligence, telecommunications and internet data to X-Keyscore database;[7]
b. Intercepting the SEA-ME-WE-3 fibre-optic cable that runs from Japan to Northern Germany, thus accessing and monitoring much of Asia's telecommunications and internet traffic with Europe;[8] and
c. Collecting email and instant messenger address databases.[9]

18. With the publication on 2 December 2013 by *The Guardian* of a leaked 2008 Five Eyes memorandum, it is also evident that the ASD proposed sharing "bulk, unselected, unminimised metadata as long as there is no intent to target an Australian national. Unintentional collection is not viewed as a significant issue."[10] This may include sensitive data such as "medical, legal, religious or restricted business information."

19. The ASD is thus collecting, sharing and receiving massive amounts of private data in an environment where little transparency and accountability is brought to bear. This in itself raises concerns of impropriety and warrants investigation by the Inspector-General. Moreover, it is now plainly obvious that the ASD is sharing the data of Australian persons in a manner that contravenes the ASD's Rules to Protect the Privacy of Australians and circumvents the requirements for ministerial authorization contained in section 9 of the ISA. In this context, the ASD is in violation of section 12 of the ISA, which prescribes that "an agency must not undertake any activity unless the activity is necessary for the proper performance of is functions; or authorized or required by or under another Act."

20. Accordingly, the Inspector-General should investigate the acts or practices of the ASD to verify whether they are in compliance with the laws and rules that regulate the agency and otherwise meeting the requisite standard of propriety.

Request for access to documents

21. We note that the Inspector-General has the power to request access to documents relevant to the investigation under section 18 of the IGIS Act. We re-

---

[7] Snowden reveals Australia's links to US spy web, The Age, 8 July 2013, accessible at http://www.theage.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html

[8] Australian spies in global deal to tap undersea cables, The Sydney Morning Herald, 29 August 2013, accessible at http://www.smh.com.au/technology/technology-news/australian-spies-in-global-deal-to-tap-undersea-cables-20130828-2sr58.html

[9] Australia collecting data for NSA, leaks show, The Sydney Morning Herald, 16 October 2013, accessible at http://www.smh.com.au/it-pro/security-it/australia-collecting-data-for-nsa-leaks-show-20131015-hv24k.html

[10] Revealed: Australian spy agency offered to share data about ordinary citizens, The Guardian, 2 December 2013, accessible at http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens

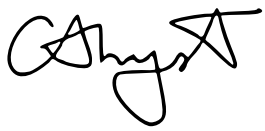
spectfully request you obtain and provide copies of any and all records pertaining to, relating to, appended to, amending, governing or extending the British-United States Communications Intelligence Agreement (now known as the UKUSA Agreement, also referred to as the Five Eyes Agreement) and subsequent instruments or other documents constituting agreements regarding the exchange of communications intelligence between the Australian government and the United States, New Zealand, Canada and the United Kingdom.

22. We previously requested copies of such records from the Department of Foreign Affairs and Trade, the Department of Defence and the Prime Minister and Cabinet on 26 November 2013. On 2 December 2013, we were informed by Rod Duffield, Director of Freedom of Information of the Department of Defence, that all departments were exempt from responding to our requests by virtue of section 7 (2A) of the *Freedom of Information Act 1982*. I enclose a copy of Mr. Duffield's correspondence for your perusal.

Further correspondence

23. Please forward any further correspondence to the author at carly@privacy.org. Please don't hesitate to contact us should you require any further information. We look forward to your prompt response.

Sincerely,



Carly Nyst
Privacy International

From: **Dudfield, Rod MR** rod.dudfield@defence.gov.au
Subject: Freedom of information request [SEC=UNCLASSIFIED]
Date: 2 December 2013 02:43
To: Carly Nyst carly@privacy.org
Cc: FOI FOI@pmc.gov.au, foi@dfat.gov.au, FOI FOI@defence.gov.au

UNCLASSIFIED

Good afternoon Ms Nyst,

I refer to your email below, received by the Australian Department of Defence on 27 November 2013, in which you seek documents under the *Freedom of Information Act 1982* (FOI Act), specifically:

> **ITEM 1** - copies of any and all records pertaining to, relating to, appended to, amending, governing or extending the British-United States Communications Intelligence Agreement (now known as the UKUSA Agreement, also referred to as the Five Eyes Agreement) and subsequent instruments or other documents constituting agreements regarding the exchange of communications intelligence between the Australian government and the United States, New Zealand, Canada and the United Kingdom.

In regard to your request I have confirmed that the records you seek relate to the operation of the Australian Signals Directorate (also known as the Defence Signals Directorate). In accordance with subsection 7(2A) of the FOI Act [Exemption of certain persons and bodies], ASD is a listed agency exempt from the operation of the FOI Act and therefore your application is not subject to the FOI Act.

I note also that you have made the same application to the Department of Prime Minister and Cabinet and Department of Foreign Affairs and Trade. In this regard the Guidelines issued by the Australian Information Commissioner under s 93A of the *Freedom of Information Act 1982* (The Guidelines) stipulates that requests for documents that may be subject to exclusion from operations of the FOI Act must be transferred to the portfolio department responsible for the exempt agency or body. On this basis please accept this response on behalf of all agencies to which you have made application. A copy of the relevant sections of the Guidelines is provided below:

> ***Mandatory transfer of requests***
>
> 2.14 Certain FOI requests must be transferred to another agency. Where an agency or a minister receives a request for access to a document which:
>
> - originated with or was received from an exempt agency or body listed in paragraph 2.9 above, and
> - is more closely connected with the functions of that exempt agency or body than with those of the agency receiving the request
>
> the request must be transferred to the portfolio department responsible for the exempt agency or body (s 16(2)).
>
> ***Responding to access requests if an exemption applies***
>
> 2.16 Where an agency is exempt in whole from the FOI Act because of s 7, it is not obliged to respond to requests for access to documents or amendment or annotation of personal records. It is nevertheless good administrative practice for an exempt agency to reply to an applicant stating that the agency is not subject to the FOI Act.

The *Guidelines issued by the Office of the Australian Information Commissioner* are available online at www.oaic.gov.au/publications/guidelines.html and the FOI Act is available at www.comlaw.gov.au/Details/C2012C00231.

I regret that I can therefore be of no further assistance to you in this matter.

Regards

Rod Dudfield
Director Freedom of Information
Ministerial and Information Management Branch
Department of Defence

Phone: 02 6266 3754

E-mail: rod.dudfield@defence.gov.au <mailto:rod.dudfield@defence.gov.au>

IMPORTANT: This email remains the property of the Department of Defence and is subject to the jurisdiction of section 70 of the Crimes Act 1914. If you have received this email in error, you are requested to contact the sender and delete the email.

From: Carly Nyst [mailto:carly@privacy.org]
Sent: Wednesday, 27 November 2013 00:13
To: FOI
Subject: Freedom of information request

Dear Sir/Madam,

Please find attached a request under the Freedom of Information Act 1982.

We would greatly appreciate it if you could confirm receipt of this correspondence.

Kind regards,

Carly Nyst

Head of International Advocacy
Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

E: carly@privacy.org
W: www.privacyinternational.org
T: +44 (0)203 422 4321
M: +44 (0) 7788 286 389

Privacy International is a registered charity (No. 1147471).
To donate please visit https://www.privacyinternational.org/donate

---

