

2 December 2013

Professor Gillian Triggs
President, Australian Human Rights Commission
GPO Box 5218
Sydney NSW 2001
Australia
By email: complaintsinfo@humanrights.gov.au

Dear Professor Triggs,

Re: Referral to the Inspector-General of Intelligence and Security

1. We write to respectfully request that the Australian Human Rights Commission refer the practices of the Australian Signals Directorate to the Inspector-General of Intelligence and Security under section 8(2)(a)(iv) of the *Inspector-General of Intelligence and Security Act 1986* (hereafter "IGIS Act").
2. We note that the Act allows the Inspector-General to inquire into the practices of the Australian Signals Directorate (hereafter "ASD") that "may be inconsistent with or contrary to any human right, that constitutes or may constitute discrimination, or that is or may be unlawful under the *Age Discrimination Act 2004*, the *Racial Discrimination Act 1975*, or the *Sex Discrimination Act 1984*," provided it is referred to the Inspector-General by the Australian Human Rights Commission.
3. We contend that the practices of the ASD, and indeed the legislation governing the operation of the ASD, contravene the right to privacy enshrined in Article 17 of the *International Covenant on Civil and Political Rights*, and the prohibition against unlawful discrimination in section 9(1) of the *Racial Discrimination Act 1975*.
4. While we appreciate that there is no formal mechanism through which we can request that the Australian Human Rights Commission submit a referral to the Inspector-General, we hope that this communication will suffice. We have set out below the practices of the ASD that raise human rights concerns.
5. In addition, we attach a complaint submitted today to the Inspector-General directly on behalf of the author, an Australian citizen, which pertains to the activities of the ASD that we believe to be contrary to the laws of the Commonwealth.

The right to privacy

6. It is understood that Australia, as part of the Five Eyes intelligence-sharing alliance with the United Kingdom, the United States, Canada and New Zealand, is collecting massive amounts of communications and communications metadata and sharing it fluidly with intelligence agencies around the world. This was confirmed today when, as part of a series of leaks by ex-NSA whistleblower Edward Snowden, a memo was released that reveals that the ASD proposed sharing “bulk, unselected, unminimised metadata” with its Five Eyes partner counterparts, including sensitive data such as “medical, legal, religious or restricted business information.”¹ Previous Snowden leaks have confirmed that the ASD is contributing such intelligence to the X-KEYSCORE database;² intercepting the SEA-ME-WE-3 fibre-optic cable that runs from Japan to Northern Germany, thus accessing and monitoring communications much of Asia’s telecommunications and internet traffic with Europe;³ and collecting email and instant messenger address databases.⁴
7. These mass surveillance activities are a violation of the internationally-recognised right to privacy.
8. Article 17 (1) of the International Covenant on Civil and Political Rights, to which Australia is a party, provides:

“No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”

9. According to the United Nations Human Rights Committee, in its General Comment No. 16:

“Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.”⁵

¹ 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>

² 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>

³ 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>

⁴ 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>

⁵ CCPR General Comment No. 16: Article 17 (Right to Privacy), para. 8.

10. The Committee acknowledges that interferences may only occur where relevant legislation specifies in detail the precise circumstances under which interferences are permitted, and where a decision to authorize interference is made by a designated authority on a case-by-case basis. The UN Special Rapporteur on the right to freedom of opinion and expression has more recently⁶ further elaborated upon the Committee's reasoning and described in detail the requirements that must be met to justify interferences with the right to privacy. These include that interferences are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application; are strictly and demonstrably necessary to achieve a legitimate aim; and adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted.

11. The Special Rapporteur went on to address whether mass interception of fibre optic cables could meet such strict requirements:

“By placing taps on the fibre optic cables, through which the majority of digital communication information flows, and applying word, voice and speech recognition, States can achieve almost complete control of tele- and online communications.”⁷

12. The Special Rapporteur further states that this kind of

“[m]ass interception technology eradicates any considerations of proportionality, enabling indiscriminate surveillance. It enables the State to copy and monitor every single act of communication in a particular country or area, without gaining authorization for each individual case of interception.”⁸

13. Mass surveillance has also been found to be an interference with the right to privacy under European human rights law. Article 8 of the European Convention on Human Rights provides a right to respect for one's “private and family life, his home and his correspondence”, subject to certain restrictions that are “in accordance with law” and “necessary in a democratic society”. The European Court of Human Rights has consistently held that the surveillance of telephone communications content by State authorities constitutes an interference with Article 8,⁹ and this undoubtedly extends to facsimile and e-mail communications content.¹⁰ In *Weber and Saravia v Germany* (2006) Application 54934/00, the Court reiterated that

⁶ Report of the Special Rapporteur on freedom of expression and opinion, Frank La Rue, 17 April 2013, A/HRC/23/40.

⁷ At para 38.

⁸ At para 62.

⁹ See *Malone v United Kingdom* (1985) 7 EHRR 14 [64]; *Weber v Germany* (2008) 46 EHRR SE5 at [77]; and *Kennedy v United Kingdom* (2011) 52 EHRR 4 at [118].

¹⁰ *Liberty & Ors v United Kingdom* (2008) Application 58243/00

“the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants’ rights under Article 8, irrespective of any measures actually taken against them”.

14. The collection and storage of data that relates to an individual’s private life is so invasive, and brings with it such risk of abuse, that it alone amounts to an interference with the right to privacy, according to European Court of Human Rights jurisprudence.¹¹ The subsequent use of the personal information has no bearing on whether its collection and storage constitutes an interference with the right to privacy.

15. By undermining the enjoyment of the right to privacy, mass surveillance, interception and collection of data also interferes with the right to freedom of expression. The UN Special Rapporteur, in a previous report on the right to freedom of expression and the internet, emphasised that “[t]he right to privacy is essential for individuals to express themselves freely,” and observed that the monitoring and collection of information about individuals’ communications and activities on the internet

“can constitute a violation of the Internet users’ right to privacy, and, by undermining people’s confidence and security on the Internet, impede the free flow of information and ideas online.”¹²

16. In his later report on privacy, the Special Rapporteur went on to note:

“States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are inter-linked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States’ scrutiny.”¹³

17. The ASD is clearly complicit in mass surveillance activities that violate the right to privacy. In this context, we believe it is imperative that the Australian Human Rights Commission refer the matter to the Inspector-General for immediate investigation.

¹¹ *S and Marper v United Kingdom* (2009) 48 EHRR 50 at [67].

¹² A/HRC/17/27, at para. 53

¹³ A/HRC/23/40, at para. 79.

Unlawful discrimination on the basis of nationality

18. A defining feature of surveillance laws in each of the Five Eyes countries is a distinction between domestic and foreign intelligence, internal and external communications, or the rights of nationals and non-nationals. By manipulating these distinctions and applying different legal thresholds to the two categories, Five Eyes members are purporting to meet their human rights obligations to respect and protect communications privacy. Yet, we now know, the Five Eyes states are subsequently sharing the vast majority of signals intelligence collected through their foreign intelligence operations with other members of the alliance. Accordingly, they are circumventing their obligations in a way that insulates them from criticism or complaint and yet continues to imperil the rights of their citizens.
19. Just like the other Five Eyes States, Australia provides a higher threshold and set of safeguards for the rights of Australian persons than for non-Australian persons. With respect to the former, a full set of *Rules to Protect the Privacy of Australians* applies pursuant to section 15 of the *Intelligence Services Act* (hereafter “the ISA”), as does a requirement for prior ministerial authorization under section 9 of the same Act. With respect to the collection of intelligence on non-Australian persons, however, no safeguards apply. The ASD may perform any activity and collect intelligence without restraint provided it does so within the confines of its functions, prescribed by section 7 of the ISA.
20. The provisions of the ISA thus distinguish between the protections afforded to nationals of Australia, and the protections afforded to the nationals of any other country. This infringes Australia’s obligations to ensure all persons under their jurisdiction are entitled to the equal protection of human rights and free from unlawful discrimination on the basis of nationality.
21. In human rights law, discrimination constitutes any distinction, exclusion, restriction or preference, or other differential treatment based on any ground, including national or social origin, or other status, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment, or exercise by all persons, on an equal footing, of all rights and freedoms. The Human Rights Committee has deemed nationality a ground of “other status” with respect of article 2(1) of the ICCPR in *Gueye and ors v France*,¹⁴ and indeed this is reflected in domestic Australian law, which prohibits unlawful discrimination on the basis of nationality in the *Racial Discrimination Act*.
22. It is both irrational and contrary to the spirit and purpose of international human rights norms to suppose that the privacy of a person’s communications could be accorded different legal weight according to their nationality or residence. If an individual within a State’s jurisdiction is granted lower or diminished human rights protections – or indeed is deprived of such protections – solely on the basis of her nationality or location, this will not only lead to a vio-

¹⁴ *Gueye and Others v. France* (Comm. No. 196/1985)

lation of the right she seeks to enjoy, but will amount to an interference with her right to be free from discrimination.

23. Where the ASD interferes with the communication of an individual in Australia, regardless of where the individual is, that individual is brought within the jurisdiction of Australia. Accordingly, Australia owes human rights obligations, and in particular the obligation to prohibit unlawful discrimination, to that individual.

24. In this context, we believe it is important that the Australian Human Rights Commission refer to the Inspector-General the question of whether the ISA or the practices of the ASD infringe the *Racial Discrimination Act* or other human rights norms.

Further correspondence

25. 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

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 DSD¹ 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 cooperation 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.pdf Intelligence'

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 its 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,

A handwritten signature in black ink, appearing to read 'Carly Nyst', with a stylized flourish at the end.

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>

