PRIVACY INTERNATIONAL

62 Britton Street
London, EC1M 5UY
United Kingdom
T +44 (0) 203 422 4321
info@privacy.org
www.privacyinternational.org

7th February 2014

Privacy International respectfully submits the following statement in response to the Intelligence and Security Committee's (ISC) call for evidence relevant to its inquiry into the laws that govern the intelligence agencies' ability to intercept private communications.

Executive Summary

This submission is confined to addressing the question, posed by the ISC, of *"Whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit for purpose', given the developments in information technology since they were enacted."*

While evolving technology has rendered the current legal framework deficient in numerous ways, this submission focuses on two particular shortcomings that have not received as much attention as they deserve.

I. First, since the late 1940s the United Kingdom has been sharing and receiving intelligence from its partners in the Five Eyes alliance – the United States, Canada, Australia and New Zealand. In recent years, this information sharing has reportedly increased significantly as the Fives Eyes have rapidly developed their technological ability to obtain and share massive amounts of data. Yet the agreements between these States governing intelligence sharing remain secret, and current UK law places no meaningful restrictions on the information that the intelligence and security services can share with and obtain from this network. This lack of a clear and foreseeable legal regime governing Five Eyes data sharing is a violation of the European Convention on Human Rights (ECHR), and requires immediate reform.

II. Second, the Regulation of Investigatory Powers Act 2000 (RIPA) contravenes the ECHR by prescribing differential standards for the interception of external, as opposed to internal, communications, providing a framework whereby the former can be intercepted and

retained en masse. This disparate treatment not only violates the privacy of those whose communications are interfered with, it discriminates against non-UK nationals in violation of Article 14 of the ECHR. Given the nature of modern communications, which may be routed and intercepted anywhere in the world without the sender's knowledge, such discrimination is neither reasonable nor justifiable.

These two elements of the current legal framework governing intelligence activities render it unfit for purpose in the modern digital era.

I. UK Security and Intelligence Agencies' Access to Information Collected by Their Partners in the Five Eyes Network Is Inadequately Regulated

1. In recent years, we have learned of a number of programmes through which the UK intelligences agencies gain access to information collected by their partners in what has commonly become known as the Five Eyes alliance. The intelligence agencies involved in that alliance are the United Kingdom's Government Communications Headquarters (GCHQ), the United States National Security Agency (NSA), Canada's Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB).

2. Conceived in 1946, the alliance developed through a series of bilateral agreements over more than a decade that became known as the UKUSA agreement. The primary purpose of the Five Eyes alliance is the sharing of signals intelligence (hereafter "SIGINT"). While the existence of the alliance has been noted in history books, and references are often made to it as part of reporting on the intelligence agencies, there is little knowledge or understanding outside the services themselves of exactly what the arrangement comprises and the rules that govern the sharing of information between its parties.

3. The close relationship between the Five Eyes is evidenced by documents recently released by Edward Snowden. Almost all of the documents include the classifi-

cation "TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL." These markings indicate the material is top-secret communications intelligence (aka SIGINT) material that can be released to the UK, the US, Australia, Canada and New Zealand. The purpose of the REL TO is to identify classified information that a party has predetermined to be releasable (or has already been released) through established foreign disclosure procedures and channels, to a foreign country or international organisation.[1]

4. The relationship between the NSA and GCHQ appears to be particularly intimate. A senior member of Britain's intelligence community described the relationship thus:

> When you get a GCHQ pass it gives you access to the NSA too. You can walk into the NSA and find GCHQ staff holding senior management positions, and vice versa. When the NSA has a piece of intelligence, it will very often ask GCHQ for a second opinion. There have been ups and downs over the years, of course. But in general, the NSA and GCHQ are extremely close allies. They rely on each other.[2]

5. 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 between the UK and the US means "that SIGINT customers in both capitals seldom know which country generated either the access or the product it-

---

[1] Security Classification Markings—Authorization for Release To (RELTO) and Dissemination Control/ Declassification Markings, USTRANSCOM Foreign Disclosure Office, available at: http://www.transcom.mil/publications/showPublication.cfm?docID=04A4D891-1EC9-F26D-0715CB3E5AF1309B

[2] Nick Hopkins, "From Turing to Snowden: how US-UK pact forged modern surveillance," 2 December 2013, available at: http://www.theguardian.com/world/2013/dec/02/turing-snowden-transatlantic-pact-modern-surveillance?CMP=twt_gu.

[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

self."[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]

6. GCHQ's access to NSA programmes such as Prism[6] and Dishfire[7] is emblematic of the types of information that is shared with the UK intelligence agencies. Despite the reported prevalence of such sharing, there is no clear publically accessible guidance in UK law regarding how and when the intelligence and security services can access information collected by their partners.

7. To begin with, the myriad of agreements that govern Five Eyes sharing remain secret. Indeed, not only are the public unable to access and scrutinise the agreements that regulate the actions of the Five Eyes, but even the intelligence services themselves do not have a complete picture of the extent of intelligence sharing activities. The NSA admitted during legal proceedings in 2011 that the information-gathering infrastructure was so complex that "there was no single person with a complete understanding."[8]

---

[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, 18th November, 2013, available at: http://www.japantimes.co.jp/news/2013/11/18/world/britains-gchq-the-brains-americas-nsa-the-money-behind-spy-alliance/#.UozmbMvTnqB

[6] Nick Hopkins, "UK gathering secret intelligence via covert NSA operation," The Guardian, 7 June 2013, available at: http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism; ISC, "Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme," available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf.

[7] James Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep," The Guardian, 16 January 2014, available at: http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

[8] Iain Thompson, "Declassified documents show NSA staff abused tapping, misled courts," The Register, 11 September 2013, avail-

8. The domestic legal framework governing Five Eyes sharing is equally obfuscated. This Committee responded to the Snowden revelations regarding Prism by remarking:

> It has been alleged that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications […] and we are satisfied that they conformed with GCHQ's statutory duties. The legal authority for this is contained in the Intelligence Services Act 1994.[9]

9. Yet the chair of this Committee has in fact admitted, there is confusion about whether "if British intelligence agencies want to seek to know the content of emails can they get round the normal law in the UK by simply asking an American agencies to provide that information?"[10]

10. A former member of the cabinet and the National Security Council has expressed concerns that UK law may not clearly address or proscribe such "jurisdiction-swapping."[11]

11. This confusion in understandable given that the current UK legal regime provides no effective guidance on the circumstances in which, and the conditions on which, the security and intelligence agencies may obtain intelligence from their Five Eyes partners. The cited

---

able at: http://www.theregister.co.uk/Print/2013/09/11/declassified_documents_show_nsa_staff_abused_tapping_misled_courts/

[9] ISC, "Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme," available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf

[10] Nicholas Watts, "GCHQ 'broke law if it asked for NSA intelligence on UK citizens', The Guardian, 10 June 2013, available at: http://www.theguardian.com/world/2013/jun/10/gchq-broke-law-nsa-intelliegence

[11] Chris Huhne, "Prism and Tempora: the cabinet was told nothing of the surveillance state's excesses," The Guardian, 6 October 2013, available at: http://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet-surveillance-state.

Intelligence Services Act 1994 (ISA) is merely a broad, vague law that fails to set out minimum safeguards, or provide details of or put restrictions upon the nature of intelligence sharing.

12. Section 3(1) of the ISA describes the functions of GCHQ in these terms:

> (1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be –
>
> (a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and
>
> (b) to provide advice and assistance [...]"

13. Section 3(2) of the ISA specifies the purposes for which the functions referred to in s3(1)(a) shall be exercisable, and makes clear that they shall be exercisable only -

> (a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
>
> (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or
>
> (c) in support of the prevention or detection of serious crime.

14. Section 4(2)(a) of the ISA imposes on the Director of GCHQ a duty to ensure –

> (a) that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal pro-

ceedings.

15. An analysis of these cursory legal provisions reveals that they fall far short of describing the fluid and integrated intelligence sharing activities that take place under the ambit of the Five Eyes arrangement with sufficient clarity and detail to ensure that individuals can foresee their application. As such, the UK regime violates the requirements that any infringement on the right to privacy be in accordance with law and necessary in a democratic society pursuant to Article 8 of the ECHR.

16. We can look to a significant body of European Court of Human Rights jurisprudence for guidance on what constitutes interference "in accordance with the law" in the context of secret surveillance and information gathering, such as that undertaken by the Five Eyes.

17. The Court begins from the perspective that surveillance, particularly secret surveillance, is a significant infringement on human rights, and in order to be justified under the ECHR must be sufficiently clear and precise "to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference."[12]

18. It must be clear "what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive," and the law must indicate "with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities"[13] in order that individuals may have some certainty about the laws to which they are subject and regulate their conduct accordingly.

19. Yet "the degree of certainty will depend on the circumstances."[14] As the Court has noted, "foreseeability

[12] Malone v United Kingdom (1985) 7 EHRR 14 [67]
[13] Ibid, at [79].
[14] Ormerod., R. and Hooper, Blackstone's Criminal Practice 2012, London 2012.

in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly..." [15]

20. Where a power vested in the executive is exercised in secret, however, the risks of arbitrariness are evident: in the words of the Court in *Weber v Germany,* "a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it." [16] In such circumstances, "is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated…" [17]

21. The Court's decision in *Weber* gave substance to this requirement:

> In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.[18]

22. The ISA fails to set out the circumstances in which the intelligence agencies can obtain information acquired by another Five Eyes party, except to vaguely require such sharing be "necessary for the proper discharge" of GCHQ's functions. Similarly, the circumstances un-

[15] Weber v Germany, Application 54934/00, (2008) 46 EHRR SE5 at [77.]
[16] Ibid, at [106].
[17] Kruslin v France (1990) 12 EHHR 547, at [33].
[18] Ibid, at [95]

der which the UK agencies can request the interception of communications by another party to the alliance are not circumscribed. There is no adequate legal regime indicating the procedure for receipt, examination, use and transfer to third parties of the shared information. Together, these deficiencies demonstrate that the UK intelligence agencies' access to and processing of information obtained by their Five Eyes partners falls far short of being in accordance with law.

II. RIPA's Discrimination Between UK Nationals and Non-Nationals is a Violation of the ECHR

23. With the advent of the internet and new digital forms of communication, now most digital communications take the fastest and cheapest route to their destination, rather than the most direct. The design and infrastructure of the internet means that the sender has no ability to choose, nor immediate knowledge of, the route that his communication will take. Even when a digital communication is being sent to a recipient within the same country as the sender, it may travel around the world to reach its destination.

24. This development in communications infrastructure means that communications travel through many more countries, are stored in a variety of countries (particularly through the growing popularity of cloud computing), and are thus vulnerable to inception by multiple intelligence agencies. While there are many methods used by intelligence agencies, including those in the UK, to intercept communications, one of the consistent techniques employed is the exploitation of the communications infrastructure itself, often in the form of attaching probes to the transnational undersea fiber optic cables that carry the world's communications.

25. According to recent reports, the UK intelligence agencies are intercepting, storing and processing communications that enter and exit the country via a mass surveillance programme code-named Tempora. Due to the UK's geographical position, a disproportionate number of undersea cables land in the UK before they cross the

Atlantic Ocean. The Guardian[19] reported that by the summer of 2011, GCHQ had attached probes to more than 200 links within UK territory, including at main network switches and undersea cable landing stations.

26. Crucially, by intercepting communications in this way, UK agencies are interfering with each communication within UK territory. Such interference violates the right to privacy and must be justified in accordance with the UK's obligations under the ECHR.

27. Pursuant to the ECHR, regardless of their location or nationality, all individuals are entitled to have their right to privacy respected not only by the State upon whose territory they stand, but by the State within whose territory their rights are exercised. If their communications pass through the territory of another State, and that State interferes with the communications, it will activate that State's jurisdiction. Accordingly, the UK owes the same obligation to each individual whose communications pass through its territory: not to interfere with those communications, subject to permissible limitations established under international law.

28. This conclusion is founded in Article 1 of the ECHR, which holds that: "*The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.*" The European Court of Human Rights has accepted that an individual may be within a contracting state's jurisdiction even if the individual is not physically present in the state's territory, so long as the individual's right was violated within the territory.

29. For example, in *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi v Ireland* (2005) 42 EHRR 1, Irish authorities at Dublin Airport impounded an aircraft that had been leased by a Turkish company. The company

[19] Ewan MacAskill et al., "GCHQ taps fibre-optic cables for secret access to world's communications," The Guardian, 21 June 2013, available at: http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

argued that the Irish authorities had acted in a way that was incompatible with the ECHR. In considering the issue of jurisdiction, the Court noted the territorial basis of jurisdiction in international law and observed:

> In the present case it is not disputed that the act about which the applicant company complained, the detention of the aircraft leased by it for a period of time, was implemented by the authorities of the respondent State on its territory following a decision made by the Irish Minister for Transport. In such circumstances the applicant company, as the addressee of the impugned act, fell within the 'jurisdiction' of the Irish State, with the consequence that its complaint about that act is compatible ratione loci, personae and materiae with the provisions of the Convention (at [para. 137]).

30. Accordingly, when intercepting communications in their territory, UK intelligence agencies are obligated to act in a manner that is compatible with the ECHR, no matter where the sender or recipient of the communication is located.

31. Contrary to this jurisprudence, RIPA enshrines a discriminatory regime that disproportionately impacts non-UK nationals. That regime is both a violation of Article 8 and Article 14 of the ECHR. Specifically, RIPA distinguishes between "internal" and "external" surveillance. Where the communication is internal (i.e. neither sent nor received outside the British Islands, see RIPA s 20), a warrant to permit lawful interception must describe one person as the "interception subject" (s 8(1)(a)) or identify a "single set of premises" on which the interception is to take place (s 8(1)(b)). The warrant must set out "the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted" (s 8(2)).

32. Where the communication is "external" – that is, it is either sent or received outside the British Islands – RIPA s 8(1) and 8(2) do not apply (s8(4)). There is no need to identify any particular person who is to be

subject of the interception or a particular address that will be targeted. RIPA therefore appears to legitimate the bulk interception of external communications. Such interception cannot be claimed to be a proportionate interference with the right to privacy, and thus contravenes Article 8.

33. Furthermore, the communications of non-UK nationals located outside the UK are by definition more likely to be subject to interception than those originating from UK nationals who are both located in and more likely to communicate solely within the British Islands. There is no reasonable basis for this discrimination, as it appears that pursuant to Tempora and similar programmes the UK has the same control over those communications that travel outside its borders as it does over those communications that remain within the British Islands.

34. Once collected, external communications are also more likely to be targeted for review. RIPA s16 places additional limits on the circumstances in which the communications of a person "*known to be for the time being in the British Islands*" may be "*read, looked at, or listened to.*" No such controls are placed on the examination of the communications of those outside the British Islands. A non-UK national's communications, once intercepted, are thus also more likely to be accessed, compounding the disproportionate effect of the law. There is no reasonable basis for this distinction, as the communications subject to review at this stage are all within the equal control of the UK intelligence agencies. RIPA's discrimination against non-UK nationals is thus a violation of Article 14 of the ECHR.

Privacy International thanks the Committee for its consideration of this evidence and is willing to provide further information on these topics if the Committee so desires.