GCHQ

Head of Information Legislation Team
A3J
GCHQ
Hubble Road
Cheltenham, Gloucestershire
GL51 0EX

Liberty
26 - 30 Strutton Ground
London
SW1P 2HR

GCHQ Reference: D7232/9544

Date: 13 November 2017

Dear Ms Spurrier,

I am writing in response to your letter of 19 May 2017, which seeks material concerning the sharing of information with foreign intelligence agencies. The Director, Jeremy Fleming, has asked me to respond on his behalf.

Whilst the nature of intelligence work means that we cannot reveal publicly everything that we do, as an organisation we set great store by being as open as is possible about our activities where it would not damage the public interest. That said, GCHQ's work must often be carried out in secret, covertly and is highly sensitive. Disclosure of information may, dependent on the information in question, be highly damaging to national security and to our important working relationship with partner intelligence agencies in other countries. Those public interests are reflected in the specific exclusion of GCHQ from the list of government departments in s.84 of the Freedom of Information Act ("FOIA"); its exclusion from the list of public authorities in Schedule 1 of FOIA; and its inclusion in the list of security bodies subject to the absolute exemption for national security contained in s.23 FOIA.

Information, where not in the public domain, will be retained by GCHQ under section 3(4) of the Public Records Act 1958. This does not negate GCHQ's responsibility under the 1958 Act to select records appropriately and to preserve them on behalf of The National Archives until their sensitivity diminishes and they can be released (as you observe, such release occurred in relation to earlier intelligence sharing agreements with the USA). That is, of course, an important factor to take into account when considering whether information the disclosure of which would currently be damaging to the public interest should be released at the present time.

With the above general considerations in mind, I turn to address your specific requests under paragraphs 1 and 2 at the end of your letter.

Paragraph 1: arrangements with foreign countries concerning the sharing of information

I am able to acknowledge publicly that GCHQ has a range of international partnerships aimed at protecting our national security, including on cyber security and intelligence, in line with broader UK foreign policy.

Some of our partnerships are decades old and well established, while others are developing in response to the changing threat environment. Our collaboration with the USA dates back to World War II and continues to deliver enormous benefits to both nations. The USA remains the UK's pre-eminent intelligence partner. Also well known is the broader Five Eyes relationship comprising Australia, Canada, New Zealand and the USA (in addition to the UK). However, the threats we face are increasingly global and to tackle these effectively requires international collaboration and information sharing on a greater scale than ever before.

We combat threats to the UK from terrorism, cyber-attack and serious crime - to name but a few - by working closely with partners who share our interests and face similar challenges, benefiting from their expertise, unique intelligence or regional perspectives. We share our own expertise and intelligence to better equip our international partners to combat threats in their regions, in the knowledge that threats to UK national security are not confined to our physical borders.

When it comes to intelligence and cyber endeavours to protect our national security the UK cannot work in isolation. We are good at what we do; but the best results come from combining our intelligence and expertise with that from our international partners.

As your letter acknowledges, there is some information in the public domain about our international agreements. Historical documents relating to the UKUSA agreement have been in the public domain since 2010, when they were released by GCHQ to The National Archives. The agreement provides for the exchange of "foreign communications" information and operational methods between the US and UK. The Sigint agencies of Canada, Australia and

New Zealand became parties to the agreement by virtue of arrangements in place in appendices to the agreement, which are also available at the National Archives. I enclose the relevant documents with this letter.

That said, it is vital that the specific details of current intelligence sharing arrangements between GCHQ and its partners are kept secret, in order to avoid revealing damaging information about existing intelligence gathering capabilities and relationships, and any gaps or shortcomings in those capabilities and relationships. Without such secrecy, the effectiveness of those arrangements would be severely compromised, and GCHQ would be less able to acquire and make productive use of vital intelligence that is needed to protect the UK's citizens. Hostile individuals would be able to, and would, use the information to adapt their conduct in order to minimise the chance of any future use of intelligence sharing producing valuable information about them and their activities, degrading the ability of GCHQ to disrupt their activities and protect national security.

Moreover, the publication of the details of intelligence sharing arrangements between GCHQ and partner agencies in other countries is likely to pose acute difficulties for the liaison relationships between GCHQ and those partners. Foreign states may choose to have intelligence sharing relationships with the UK on the strict understanding that those relationships will be kept confidential. If GCHQ were obliged to disclose such relationships they would be likely to discontinue or limit those relationships, leading to the loss of vital intelligence and damage to GCHQ's reach and capabilities. Other partners may choose to share intelligence with GCHQ on the understanding that they are content to avow the fact of the intelligence sharing relationship, but not all the types of intelligence that are shared as a result (for example, in order to avoid disclosing their intelligence-gathering capabilities). If further details of those relationships were published, in breach of that understanding, they would be likely to choose to restrict the information they shared with GCHQ to those types of intelligence they were prepared publicly to avow that they acquire or otherwise limit the relationship. That, too, would reduce the quantity and quality of intelligence available to GCHQ, impeding the ability of GCHQ to perform its statutory functions.

For the above reasons, it is obviously not possible, and never could be possible, for GCHQ to share *"all agreements, memoranda of understanding, or other arrangements with foreign countries concerning the sharing of raw data and other information"*.

Nevertheless, GCHQ is currently working with various of our international partners to establish whether further information can be placed in the public domain about intelligence cooperation, including the sharing of raw data and other information, in a way which does not damage the public interest.

Paragraph 2: policies, guidelines, opinions, reports and memoranda concerning intelligence sharing

Despite the obvious limitations in what GCHQ is able to say for reasons of national security, there is a great deal of information in the public domain in respect of the circumstances in which we may share and receive information, addressing the points at subparagraphs 2(a)-(d) of your letter. I point you to particularly relevant material below.

The starting point must of course be domestic legislation. Most significant to our work (in chronological order) are the Intelligence Services Act 1994, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and, most recently, the Investigatory Powers Act 2016. GCHQ must always act in accordance with the provisions contained within that legislation.

Furthermore, as a public body, GCHQ is subject to the Padfield Principle (*Padfield v Ministry of Agriculture, Fisheries and Food* [1968] AC 997) whereby it is required as a matter of domestic public law not to deliberately circumvent legislative safeguards and mechanisms.

In addition to compliance with legislation, GCHQ is subject to various codes of practice and policies which are in the public domain.

Perhaps most pertinent to your request is the Interception of Communications Code of Practice. Section 71 of RIPA requires the Secretary of State to issue one or more codes of practice relating to the exercise and performance of the powers and duties under parts I to III of the Act. The most recent guidance is entitled '*Interception of Communications*' and was published in January 2016. I enclose a copy with this letter for your assistance.

Chapter 7 of *Interception of Communications* sets out the safeguards which apply to material that is intercepted under the authority of a warrant complying with section 8(1) or section 8(4)

of RIPA and any related communications data. As you will see, this includes the following restrictions on dissemination of intercepted material:

> "7.3. The number of persons to whom any of the intercepted material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of RIPA. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the intercepted material to carry out those duties. In the same way, only so much of the intercepted material may be disclosed as the recipient needs. For example, if a summary of the intercepted material will suffice, no more than that should be disclosed.
>
> 7.4. The obligations apply not just to the original interceptor, but also to anyone to whom the intercepted material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the intercepted material further. In others, explicit safeguards are applied to secondary recipients.
>
> 7.5. Where intercepted material is disclosed to the authorities of a country or territory outside the UK, the agency must take reasonable steps to ensure that the authorities in question have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary. In particular, the intercepted material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed." [emphasis added]

As you can see from paragraph 7.5, domestic safeguards in relation to intercepted material apply to information which is disclosed to foreign intelligence agencies and GCHQ may not share such information with another country if to do so would be contrary to this Code. The above and enclosed are therefore relevant to your enquiries.

The Code also contains a chapter entitled "*Rules for Requesting and Handling Unanalysed Intercepted Communications from a Foreign Government*". This provides as follows:

> "Application of this chapter
>
> 12.1. This chapter applies to those intercepting agencies that undertake interception under a section 8(4) warrant.
>
> Requests for assistance other than in accordance with an international mutual assistance agreement

12.2. A request may only be made by an intercepting agency to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual assistance agreement, if either:

- A relevant interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular communications because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the intercepting agency to obtain those communications; or

- Making the request for the particular communications in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the intercepting agency to obtain those communications.

12.3. A request falling within the second bullet of paragraph 12.2 may only be made in exceptional circumstances and must be considered and decided upon by the Secretary of State personally.

12.4. For these purposes, a "relevant RIPA interception warrant" means one of the following: (i) a section 8(1) warrant in relation to the subject at issue; (ii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of section 8(4)(b) of RIPA) covering the subject's communications, together with an appropriate section 16(3) modification (for individuals known to be within the British Islands); or (iii) a section 8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" covering the subject's communications (for other individuals).

Safeguards applicable to the handling of unanalysed intercepted communications from a foreign government

12.5. If a request falling within the second bullet of paragraph 12.2 is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intercepting agency according to any factors as are mentioned in section 16(2)(a) and (b) of RIPA unless the Secretary of State has personally considered and approved the examination of those communications by reference to such factors.

12.6. Where intercepted communications content or communications data are obtained by the intercepting agencies as set out in paragraph 12.2, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content and communications data must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.

12.7. All requests in the absence of a relevant RIPA interception warrant to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data) will be notified to the Interception of Communications Commissioner."

As is clear from the above, GCHQ cannot acquire such information from another country if to do so would be contrary to this Code. The above and enclosed are therefore similarly relevant to your enquiries.

You are no doubt also aware of the information that was placed in the public domain regarding the policies which apply specifically to Bulk Personal Datasets and Bulk Communications Datasets. This information was released in June 2017 as part of litigation brought by Privacy International in the Investigatory Powers Tribunal (*Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* [2016] UKIP Trib 15 110 CH). I have enclosed a copy of this information, which was attached as an Annex to the Secretary of State's skeleton argument in those proceedings. I also enclose copies of the documents referred to in that Annex.

You will see that the OPEN Bulk Personal Dataset Handling Arrangements which came into force in November 2015, for example, provides at 6.1:

"Information in bulk personal datasets held by an Intelligence Service may only be disclosed to persons outside the relevant Service if the following conditions are met:

- That the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989.
- That it is necessary to disclose the information in question in order to achieve that objective;
- That the disclosure is proportionate to the objective;
- That only as much of the information will be disclosed as is necessary to achieve that objective."

This Annex also contained detail from GCHQ's own Handling Arrangements and Compliance Guide.

Similarly, the OPEN Bulk Communications Dataset Handling Arrangements which came into force in November 2015, for example, provides at 4.4:

"4.41 The disclosure of BCD must be carefully managed to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The disclosure of an entire bulk communications dataset, or a subset, outside the Intelligence Service may only be authorised by a Senior Official or the Secretary of State.

4.4.2 Disclosure of individual items of BCD outside the relevant Intelligence Service may only be made if the following conditions are met:
- that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;
- that it is necessary to disclose the information in question in order to achieve that objective;
- that the disclosure is proportionate to the objective;
- that only as much of the information will be disclosed as is necessary to achieve that objective."

Again, the Annex also included detail from GCHQ's own Handling Arrangements and Compliance Guide. These guides all apply to GCHQ's sharing of information with other countries and are therefore relevant to your enquiries.

You may also wish to consider specific guidance which has been published in relation to detainee issues. In July 2010 the Cabinet Office produced guidance entitled '*Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*'. I enclose a copy of this guidance for your assistance. This guidance sets out the principles, consistent with UK domestic law and international law obligations, which govern the interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees. As one of the three security and intelligence agencies, this guidance must be adhered to by officers of GCHQ.

You may further be assisted by the product of the ISC's investigation into the exchange of information with overseas partners, the results of which were published in their report entitled *Privacy and Security: A modern and transparent legal framework*. The legislative basis, together with policy and practice are addressed at paragraphs 240 to 254 of that report.

The report provides significant detail of GCHQ's approach in relation to the exchange of raw intercept. It states as follows:

"248. GCHQ have explained how these arrangements work in practice using the example of requesting unanalysed interception from the US National Security Agency (NSA).

• In terms of the law:

- GCHQ are legally allowed to seek intelligence from the NSA in pursuit of their functions under the provisions of the Intelligence Services Act.

- This includes both intelligence reports (analysed and summarised intelligence) and raw intelligence (original unanalysed intercept).

- RIPA does not apply in this situation: the safeguards and processes in RIPA, including obtaining interception warrants, can only make lawful actions to which UK law applies.

• In terms of policy:

- To ensure that they comply with the Human Rights Act, GCHQ's policy is that where they seek raw intercept from the NSA they follow the procedures and observe the safeguards contained in RIPA (because RIPA has been found to be ECHR compliant). This means that the HRA 'triple test' of legality, necessity and proportionality must be met and a relevant interception warrant needs to be in place – i.e. a Minister has considered that GCHQ are authorised to carry out the interception.

- GCHQ's request to the NSA would therefore be subject to the same safeguards and scrutiny as those that would be required if GCHQ themselves were carrying out the intrusive activity.

- GCHQ have adopted this policy as 'belt and braces' – they are applying one set of human rights compliant processes to a slightly different circumstance in order to provide assurance that their dealings with foreign partners are compatible with UK human rights law.

• In terms of practice:

- GCHQ have never had to seek a warrant solely for the purposes of obtaining raw intercept from an overseas partner. This is because, in practice, GCHQ only ever request intelligence on people if they are already attempting to intercept that person's communications themselves. Their own interception requires an interception warrant authorised by a Secretary of State. Therefore, in practice there has always been an interception warrant in place for any raw intercept GCHQ have sought from their overseas partners.

Therefore, to summarise:

• in legal terms, GCHQ are permitted to seek raw intercept from partners;

• nevertheless, in policy terms, GCHQ would seek "additional" Ministerial Authorisation before doing so;

• but, in practical terms, GCHQ have always had Ministerial Authorisation in place before receiving raw intercept from partners because they were already seeking intelligence on the target themselves."

I can also state without hesitation that GCHQ may not request or otherwise acquire information from another country where GCHQ itself could not lawfully acquire the same information. This is consistent with the *Padfield* principle that I have outlined above.

As the ISC observed in their report:

> "GCHQ told the Committee that they would refuse to accept intelligence from a liaison partner if it was obtained through means that would breach UK law. In relation to the NSA (their most significant partner), they said that there is a 'very clear mutual understanding of what is acceptable in legal and policy terms and [they] would not offer material that is evidently incompatible with a partner's legal and policy requirements"

The report continued that in relation to intelligence material which had not been requested:

> "GCHQ said that when they receive unsolicited intelligence from liaison partners which relates to individuals who live in the UK, they have a Sensitive Receipt Authorisation (SRA) policy to determine whether it is appropriate to accept the material. SRAs are approved internally by a senior official and reviewed at least every six months, although the Director of GCHQ told the Committee in June 2013 that 'The Foreign Secretary has now said that he wishes to receive notice of any SRAs in real time'."

I appreciate that your request seeks, in addition to the information above and enclosed, further documentation. Whilst I am not providing this documentation I can assure you that there is a strong framework of democratic accountability and oversight that governs GCHQ's work in this field and which allows for scrutiny of this area of our work.

By way of example, section 59 of RIPA provides that the Intelligence Services Commissioner must keep under review the carrying out of any aspect of the functions of GCHQ and there is a statutory obligation to produce, and to provide to Parliament, an annual report. I enclose with this letter the *Report of the Intelligence Services Commissioner for 2015*. This report confirms that the cases which were selected for scrutiny by the Commissioner met the appropriate tests for necessity, proportionality and intrusion and concluded *"that GCHQ are doing a very difficult job well and that staff are working hard to get things right"*.

Similarly, the Intelligence and Security Committee of Parliament, established by the Intelligence Services Act 1994 and strengthened by the Justice and Security Act 2013, oversees the work of GCHQ. As I have set out above, the ISC published a specific report addressing the issues you raise in March 2015, a copy of which is enclosed with this letter alongside the Government's response.

The Intelligence Services Commissioner and the Intelligence and Security Committee are both able to undertake investigations into the specific issues raised in your letter and are able to conduct their enquiries and produce reports in a way which protects the obvious sensitivities of the underlying material. Their statutory powers of investigation are of critical importance in meeting any public concerns regarding the accountability of the security and intelligence agencies.

I trust that the above, together with the documents enclosed with this letter, is sufficiently informative. As I stated at the outset of this letter, GCHQ are committed to greater openness where possible without damage to the public interest. It is with this in mind that (as I have stated) we are currently working with our international partners to establish whether further information can be placed in the public domain about intelligence cooperation in a way which does not damage the public interest. In addition, new Codes of Practice made in accordance with the Investigatory Powers Act 2016 will shortly be published, which are material to the issues raised at paragraph 2 of your letter.

Yours faithfully,

Head of the Information Legislation Team

Head of the Information Legislation Team.