HOUSE OF COMMONS
LONDON SW1A 0AA
Tel: 0207 219 8123

Rt Hon Sir Malcolm Rifkind
Chair of the Intelligence and Security Committee
House of Commons
London
SW1A 0AA

28th January 2014

Dear Malcolm,

Thank you for the 'Call for Evidence' sent to me on 7th January inviting a written submission to consider as part of your ongoing inquiry into the laws which govern the intelligence agencies' ability to intercept private communications.

In my capacity as Chair of the All Parliamentary Group on Drones, I have obtained an independent expert opinion from Jemima Stratford QC on this subject. I enclose the advice which I invite you to accept as my submission to the ISC inquiry, with particular reference to paragraph 6(b) of the Call for Evidence and your determination of whether RIPA is 'fit for purpose'.

The Advice challenges conventional thinking that the current practice of interceptions and transfer of data by GCHQ is lawful. It raises a number of questions which, in my view, may demand attention pending review of the legislative framework as a whole.

I invite you to seek independent legal advice on the following questions at your earliest convenience. They may highlight key issues and inform the remit of your inquiry:

1. Does GCHQ carry out mass interception of 'internal' contents data between UK citizens? Is this permitted under RIPA? If not, or if the answer is not clear, what steps can the ISC take or recommend to ensure this practice is stopped pending your final report?

2. Does GCHQ carry out mass interception of 'external' contents data; if this is permitted under RIPA, is it an interference with under Article 8? If not, or if the answer is not clear, what steps can the ISC take or recommend to ensure it is stopped pending your final report?

3. Is the distinction between 'contents' and 'communications' data in RIPA still meaningful given the realities of modern internet usage

4. What changes, guidance or other restraints do the ISC recommend regarding the exercise of the very broad executive discretion in respect of external communications in particular?

5. Do the mechanisms which exist in the US for ensuring storing, destroying and use of UK data comply with UK law and policy? Can UK data be directed towards activities which are unlawful in the UK, such as drone strikes against non-combatants? If so, what steps can the ISC take or recommend to ensure that this does not happen?

6. What, if any, laws, codes or guidance exist in the UK regarding storage and use of intercepted data, other than its admissibility in court? What laws, codes or guidance apply to the transfer of data to other state bodies in the UK? What steps will the ISC take or recommend to impose fair and lawful restraint on the storage and use of such data in the UK?

7. Following the end of the Noor Khan litigation, what steps can the ISC take or recommend to protect GCHQ and other Crown officials from charges or accusations of complicity in murder when data may end up being directed towards unlawful drone strikes?

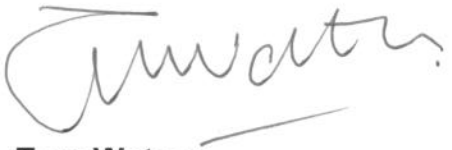
8. What steps can the ISC take to investigate the possible commission of complicity in crimes by GCHQ, other Crown officials, and visiting forces and agents? If the ISC find evidence of any possible crimes, will they pass that evidence to the DPP? To what extent can this be disclosed to the concerned British public?

9. To what extent do the ISC support the amendments, or any of them, lodged by 4 APPG peers to the Defence Reform Bill, Visiting Forces Act and RIPA which impose reporting obligations on the Interception Commissioner and others to report to the ISC? Would the amendments, or any of them, support members of the ISC in carrying out their work?

10. What steps can the ISC take to promote informed debate in parliament on all these questions at a policy level?

I hope the advice and questions posed in this letter are useful. I am happy to participate in any oral evidence session you may hold, or indeed communicate any request for Jemima Stratford QC to attend in person.

Yours sincerely



Tom Watson
Member of Parliament for West Bromwich East

Cc All members of the Intelligence and Security Committee.

IN THE MATTER OF STATE SURVEILLANCE

ADVICE

INTRODUCTION

1. We are asked to advise Tom Watson MP, Chair of the All Party Parliamentary Group on Drones, on the lawfulness of five possible scenarios concerning state surveillance in the United Kingdom.

2. The five scenarios are:
    a. The Government Communications Headquarters ('GCHQ') have intercepted bulk electronic data sent between two persons located in the UK, but transmitted along fibre-optic cables which run between the UK and the United States. The electronic data arise from internet, email and telephone use;
    b. GCHQ have retained that data and submitted it to analysis including 'pattern of life' analysis. That analysis has been applied to identified terror/criminal suspects and also to individuals who are not suspected of wrongdoing;
    c. GCHQ have permitted the National Security Agency ('NSA') of the US to access and retain that data;
    d. The NSA share data with the CIA so that it is available for targeting drone strikes;
    e. US forces operate from a UK base, under the NATO Status of Forces Agreement 1951 (for example RAF Croughton). That UK base is used as a communications hub to transfer data both to and from the US. Some of the data obtained overseas and transferred to the US have been obtained in contravention of international law. Some of the material transferred from the US via the UK includes data, instructions and orders to facilitate drone strikes.

3. The five scenarios are necessarily to some degree based on assumed facts. However, we have been referred to a number of news reports arising out of the

recent disclosures made by Edward Snowden, upon which the scenarios are based.[1] We note that in contrast to the approach of the US Government, the UK Government has refused to confirm or deny the existence of the programme outlined in the scenarios. Furthermore, the Guardian newspaper has not published any documents concerning the activities of GCHQ in connection with what is known as the TEMPORA programme.[2]

4. For the purposes of this Advice, we proceed on the basis that the five scenarios are accurate. We have been provided with copies of two applications arising from the Snowden disclosures: an application by Big Brother Watch and others to the European Court of Human Rights ('the ECtHR') (App. No. 58170/13); and an application by Privacy International to the Investigatory Powers Tribunal ('IPT'). Both of those applications proceed on the basis of matters contained in the Snowden disclosures. Furthermore, the disclosures have provided the factual under-pinning for inquiries by public bodies, including the European Parliament which has recently published a Draft Report on surveillance programmes.[3] If and when evidence substantiating or altering matters emerges, it might be necessary to re-consider relevant parts of this Advice.

5. It will be apparent that scenarios (a) – (d), and to some extent (e), are essentially sequential steps in an overall hypothetical scenario. In this Advice, we consider the legality of each scenario in turn. However, it should also be recalled that if any of the intermediate scenarios is unlawful, that will break the sequence and should prevent the authorities from acting as they currently do. In other words, the authorities must establish that every step in the chain is lawful if they are to be permitted to carry on with these activities.

---

[1] http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data; http://www.theguardian.com/uk/gchq; http://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html; http://www.independent.co.uk/news/uk/politics/exclusive-raf-croughton-base-sent-secrets-from-merkels-phone-straight-to-the-cia-8923401.html

[2] That stands in contrast to the position in the United States of America where documents demonstrating the NSA's intercept program have been published.

[3] 2013/2188 (INI) Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 8 January 2014. See, for example, the summary of the facts at para 2 on page 16.

6. We also note at the outset that the issues which we address are related to, but have a somewhat different focus from and are narrower than the issues pending before the ECtHR and the IPT in the applications referred to at paragraph 4 above. Of course, if there are any relevant developments in those proceedings, then we would need to re-visit our Advice as appropriate.

7. In summary, and for the reasons set out below:
    a. Under the Regulation of Investigatory Powers Act 2000 ('RIPA'), GCHQ is not entitled to intercept mass 'internal' contents data: the contents of emails or phone calls between two individuals located in the British Islands. GCHQ is entitled to intercept bulk 'external' contents data: the contents of communications between the British Islands and elsewhere. GCHQ is also entitled to intercept bulk communications data (sometimes termed 'metadata'). The interception of that bulk data, although lawful for the purposes of RIPA, is a disproportionate interference with the Article 8 rights of UK citizens.
    b. GCHQ is entitled to submit the mass data that they collect to pattern of life analysis, under the statutory framework. We consider that the current framework for the retention, use and destruction of communications data is inadequate and likely to be unlawful. The RIPA framework concerning external contents data is also probably unlawful;
    c. GCHQ is entitled to transfer bulk data to the NSA, under RIPA, where the Secretary of State is satisfied that the mechanisms for storing and destroying that data in the receiver country are suitable. A transfer of intercept data is a fresh interference with the individual's Article 8 rights. We consider that the statutory framework provides insufficient protections to the individuals concerned. The government could at least ameliorate that situation by agreeing and publishing a Memorandum of Understanding or other bilateral agreement on data transfer specifying how the data should be stored, when they should be destroyed, and the purposes for which the data may be used under UK law;
    d. If the UK government knows that it is transferring data that may be used for drone strikes against non-combatants (for example in Yemen or Pakistan), that transfer is probably unlawful. An individual involved in passing that information is likely to be an accessory to murder. It is well arguable, on a variety of different bases, that the government is obliged to take reasonable steps to investigate that possibility. However, it may be that the current

legislative framework imposes no obligation on the UK government to investigate or prevent its agents from becoming accessories to murder in this manner. If that is the case, we consider that outcome to be contrary to the principles of public policy and good governance;

e. The UK government is entitled to press charges against US servicemen operating from NATO bases on UK soil. If data that have been unlawfully obtained or used (for the purposes of British law) are transferred via a UK NATO base, the UK government may prosecute any US serviceman involved in that transfer. It appears, in practical terms, that the UK government may not always know what takes place on RAF bases controlled by NATO forces. As a result, that power to prosecute may be theoretical.

(A) MASS COLLECTION OF DATA

8. The statutory framework for surveillance in the United Kingdom is provided for in the Intelligence and Security Act 1994 and RIPA. RIPA is the crucial statute, for our purposes. RIPA itself relies on two essential distinctions: first, it distinguishes between 'internal' and 'external' communications; and second, it treats the interception of 'contents' and 'communications' data differently. These two distinctions are addressed in turn.

Internal and External Communications

9. RIPA provides in relevant part:

> *"1. **Unlawful interception***
>
> *(1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of–*
> *(a) a public postal service; or*
> *(b) a public telecommunication system.*
>
> ***...***
>
> *2. **Meaning and location of "interception" etc.***
> *(1) In this Act–*
> *...*
> *"public telecommunications service" means any telecommunications service which is offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom;*
> *"public telecommunication system" means any such parts of a telecommunication system by means of which any public telecommunications service is provided as are located in the United Kingdom;*

"telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service); and
"telecommunication system" means any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.

(2) For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he–
(a) so modifies or interferes with the system, or its operation,
(b) so monitors transmissions made by means of the system, or
(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

(4) For the purposes of this Act the interception of a communication takes place in the United Kingdom if, and only if, the modification, interference or monitoring ... is effected by conduct within the United Kingdom and the communication is either–
(a) intercepted in the course of its transmission by means of a public postal service or public telecommunication system; or
(b) intercepted in the course of its transmission by means of a private telecommunication system in a case in which the sender or intended recipient of the communication is in the United Kingdom.

...
5. ***Interception with a warrant.***
(1) Subject to the following provisions of this Chapter, the Secretary of State may issue a warrant authorising or requiring the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following–
(a) the interception in the course of their transmission by means of a postal service or telecommunication system of the communications described in the warrant;
...
(d) the disclosure, in such manner as may be so described, of intercepted material obtained by any interception authorised or required by the warrant, and of related communications data.
(2) The Secretary of State shall not issue an interception warrant unless he believes–
(a) that the warrant is necessary on grounds falling within subsection (3); and
(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.
(3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary–
(a) in the interests of national security;
(b) for the purpose of preventing or detecting serious crime;
(c) for the purpose of safeguarding the economic well—being of the United Kingdom; or
(d) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.
(4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any warrant shall include whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.
...

8. ***Contents of warrants.***

(1) An interception warrant must name or describe either–

(a) one person as the interception subject; or

(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.

(2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting 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.

(3) Any factor or combination of factors set out in accordance with subsection (2) must be one that identifies communications which are likely to be or to include–

(a) communications from, or intended for, the person named or described in the warrant in accordance with subsection (1); or

(b) communications originating on, or intended for transmission to, the premises so named or described.

(4) Subsections (1) and (2) shall not apply to an interception warrant if–

(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and

(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying–

(i) the descriptions of intercepted material the examination of which he considers necessary; and

(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).

(5) Conduct falls within this subsection if it consists in–

(a) the interception of ***external communications*** *in the course of their transmission by means of a telecommunication system; and*

(b) any conduct authorised in relation to any such interception by section 5(6).

(6) A certificate for the purposes of subsection (4) shall not be issued except under the hand of the Secretary of State.

...

20. ***Interpretation of Chapter I.***
In this Chapter–

...

*"****external communication****" means a communication sent or received outside the British Islands..."* (emphasis added)

10. The distinction between 'external' and 'internal' communications is critical, for the purposes of intercepting and reading the contents of communications.

11. First, the mechanism by which interception of 'internal' and 'external' communications may be authorised is different. Interception of internal communications is subject to the relatively stringent control mechanism, set out in section 8 (1) - (3) of RIPA. In particular, the warrant must identify a named person or premises.

12. Interception of external communications is much less strictly controlled. A warrant may be issued where the Secretary of State:

    a. Describes the intercepted material; and

    b. Considers that interception is necessary for the purpose of national security, preventing or detecting serious crime or safeguarding economic wellbeing.

13. Accordingly, a warrant to intercept the contents of internal communications cannot sanction the collection and retention of bulk electronic data of the sort envisaged in scenario (a). Such a warrant has to be precisely targeted to a particular person or premises.

14. The position is different in relation to 'external' warrants. Under section 8(4)(a) of RIPA, a warrant to intercept external communications only has to specify the 'communications to which the warrant relates'. For example, it might be simply that the warrant relates to interception of communications containing certain keywords. Or communications between a large number of named individuals. At the most extreme end of the spectrum, it is conceivable that an external warrant might specify 'all communications entering and leaving the British Isles', or all such communications carried on a particular cable. It may be that such broad warrants are wanted in order subsequently to carry out the keyword analysis described above.

15. In short 'external' warrants allow for interception of bulk or mass data, 'internal' warrants do not.

16. The boundary between internal and external communications is reasonably clear in most cases. Where a UK citizen sends an email or makes a telephone call to an overseas location, that is an 'external communication' (for the purposes of section 20). Assuming that the warrant was lawful in other respects (in particular, on human rights grounds), the contents of those communications could be intercepted on the section 8 (4)-(5) basis.

17. However, scenario (a) concerns the situation whereby communications between two individuals who are both based in the UK are nonetheless transmitted via a transatlantic cable. We are instructed that that may frequently occur, for example where the relevant internet server is based in the US.

18. We consider that such a communication is an internal rather than an external communication. Therefore, such communications cannot be intercepted pursuant to a section 8 (4) warrant; they may not be intercepted in bulk. The communication neither originates nor terminates outside the British Islands. Therefore it is not sent or received outside the British Islands (for the purposes of Section 20).

19. The contrary is only arguable by interposing an additional (assumed) 'sender' and 'recipient' into the chain of communication. Thus it might be argued that an email which travels from a British based computer to a US server, and then returns from the US server to another British computer, is being sent and received by the US server. We consider that this would be an artificial construction, which does not reflect the language or intention of the statutory framework.

20. The artificiality of that reasoning is exposed by the example of a mobile telephone call between two persons based in the UK. The signal may travel via a satellite, which is clearly not in the British Isles. However, if use of a satellite system makes a communication 'external', then the mobile phone system would be 'external' to the British Isles. That is certainly not what the statutory framework envisaged or intends.

21. We are reinforced in that conclusion by the Home Office Interception of Communications Code of Practice (issued pursuant to section 71 of RIPA) which states (Chapter 5 page 22):

> "*External communications are defined by the Act to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in the course of their transit.* ***They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route.***" (emphasis added)

22. That view also accords with the approach of the Court of Justice of the European Union ('the CJEU') in the analogous field of data protection. In Case C-101/01 *Lindqvist* [2003] ECR I-12971, the CJEU held that placing information on a website did not constitute transferring that data to third countries outside the EU, even if the server hosting the website was in a third country (see, in particular, paras 67-71). It is relevant to note that the finding of the CJEU was in accordance with the submissions of the UK government, which argued that there was no transfer of data outside the EU (para 55).

23. That was also the view adopted by Lord Bassam, the Parliamentary Under-Secretary for the Home Office who spoke in support of the Bill which became RIPA in the House of Lords. He encouraged other speakers to support the Bill by reference to precisely this point (HL Deb, 19 June 2000, c102):

> "*The noble Lord Phillips, made two specific points which to my mind were questions. At one stage he asked if a warrant could be treated as external merely because it was routed outside the British Islands. I have read the definition of 'external communication.' Clause 19 defines an external communication as...*

That does not mean that a communication sent and received inside the British Islands may be deemed to be external simply because it takes an international route. It must be sent or received at appoint outside the British Islands. I hope that clarifies that issue, which seemed to be of particular concern."

24. We are conscious of the limited circumstances in which it is permissible to rely on statements made in Parliament, when interpreting a statute (see *Pepper (Inspector of Taxes v Hart* [1993] A.C. 593). Nonetheless, given that the provision itself is tolerably clear and given the Home Office's view of the position, we conclude that the only credible interpretation of the statutory provisions is that the communications described in scenario (a) are internal.

25. The other possibility we have considered is that GCHQ has located the interception 'infrastructure' on a transatlantic cable in order to argue that the cable is outside of the jurisdiction. In that case, the security services might contend that the interception is "effected by conduct" outside the UK (the words used at the start of section 8(4) of RIPA) and thereby seek to evade the limitations of RIPA. We seriously doubt whether a court would accept that argument, not least because there would still be conduct connected with the interception in the UK. However, even if such an argument were successfully pursued, there would still be an issue as to whether or not the activity was lawful for the purposes of the European Convention on Human Rights ('the Convention'). We address that issue below.

26. In summary therefore, RIPA only entitles the UK security services to intercept bulk contents data where at least one party to the communication is located outside the British Isles. Thus the activities described in scenario (a) are unlawful as contrary to RIPA.

Contents and Communications Data

27. The second critical distinction within RIPA is the different treatment of 'contents' and 'communications' data. Communications data are made up of 'traffic data' and "*any information which includes none of the contents of a communication (apart from any information falling within paragraph a) and is about the use made by any person... in connection with the provision to or use by any person of any telecommunications service."* (section 21 (4) (b). 'Traffic data are defined as:

"2 (9) any data identifying or purporting to identify any person, apparatus or location to or from which the communication is or may be transmitted;
(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,

(c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and
(d) any data identifying the data or other data as data comprised in or attached to a particular communication."

Communications data are sometimes referred to as metadata, but we use the term 'communications data' since it is employed in RIPA.

28. The Act imposes many fewer restrictions on interception of communications data. They may be intercepted, pursuant to an 'authorisation' (not warrant) (section 22):

    a. *"In the interests of national security;*
    b. *For the purpose of preventing or detecting crime or of preventing disorder;*
    c. *In the interests of the economic well-being of the United Kingdom;*
    d. *In the interests of public safety*
    e. *For the purpose of protecting public health;*
    f. *For the purpose of assessing or collecting any tax...*
    g. *For the purpose, in an emergency, of preventing death or injury...*
    h. *For any purposes... which is specified for the purposes of this subsection by an order made by the Secretary of State."*

29. As with the interception of communications data, the authorisation must be proportionate to what is sought to be achieved (section 22 (5)).

30. Authorisations do not take effect until they are approved by a Justice of the Peace (section 23A). They may be made by a wide range of 'designated persons' within the police, National Crime Agency, HMRC and other bodies (sections 22-25).

31. In relation to communications data, RIPA draws no distinction between internal and external interception. Assuming that an authorisation is in other respects lawfully issued, GCHQ could obtain and retain mass communications data. There would be no reason (other than convenience) for them to do so via the transatlantic cable; they could intercept that communication on the UK mainland.

32. RIPA further imposes a number of restrictions on the manner in which contents and communications data may be held (addressed in part B below), and also contains the mechanisms by which the security services will be overseen. Part IV provides for the existence of an Information Commissioner and an Investigatory Powers Tribunal, before whom the actions of the security services may be challenged.

<u>Is the statutory framework lawful?</u>

33. The primary ground on which the lawfulness of RIPA might be challenged is in respect of the right to privacy under the European Convention for Human Rights ('ECHR'). Article 8 of the Convention provides:

> "8.1 *Everyone has the right to respect for his private and family life, his home and correspondence.*
> *8.2 There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals and for the protection of the rights and freedoms of others.*"

34. Interception of contents and/or communications data is clearly an interference with the Article 8 rights of the individual concerned. Therefore in order to be lawful, the interference must be 'in accordance with the law', pursuant to a legitimate aim and proportionate in the circumstances.

35. The requirement to be 'in accordance with the law' will not be satisfied by merely asserting that a particular act is allowed under the statutory framework. That statutory framework itself must be of sufficient 'quality'. In *Malone v United Kingdom* (Application No 8691/79), the ECtHR held that (para 67):

> "... *'in accordance with the law' does not merely refer back to the domestic law but also relates to the quality of the law requiring it to be compatible with the rule of law... there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded in paragraph 1. Especially where the power of the executive is exercised in secret, the risks of arbitrariness are evident... the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms 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 with the right to respect for private life and correspondence...*"

36. The Court concluded that the law (as then in force) was not sufficiently precise and clear as to how and when the state could lawfully exercise its powers of interception.

37. Many of the same issues were canvassed again in *Liberty v United Kingdom* (Application No. 58243/00). The case concerned the statutory framework which was in force immediately prior to the introduction of RIPA. That framework allowed for the interception of telephone calls between Ireland and the UK. The ECtHR reiterated that the requirement that a statutory framework is 'in accordance with the law', required more than simply having a basis in domestic law. It also "*refers to the quality of the law in question*" (paragraph 59). The statutory framework and guidance must be compatible with the rule of law and accessible to the individual citizen. The citizen

should be able to foresee its consequences for him. In the case of interception, where the executive's discretion is so wide, it was particularly important to have clear rules to avoid the risk of arbitrariness (para 95):

> "*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 likely 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.*"

38. The ECtHR noted that the pre-RIPA legislation gave the Secretary of State the power to warrant interception of '*such external communications as are described in the warrant.*' That was too broad a power: it led to the result that almost all external communications transmitted by submarine cables could be intercepted.[4] Furthermore, the Secretary of State exercised a wide discretion as to which of those communications should then be analysed: they were determined by reference to broad categories such as "national security." The pre-RIPA framework also failed to provide any detailed description of the arrangements made for the examination, storage and destruction of material that was intercepted. Accordingly, the ECtHR concluded that the pre-RIPA code was not sufficiently clear to provide adequate protection against arbitrary interference with the applicant's Article 8 rights.

39. RIPA itself has recently been examined by the ECtHR in *Kennedy v United Kingdom* (Application No. 26839/05). It is important to note that the case concerned the interception of the contents of an individual's internal correspondence; it did not address external communications. The Court held that:
    a. The phrases 'national security' and 'serious crime' were sufficiently clear justifications for public authorities rely on when justifying the grounds for an act of surveillance (para 159);
    b. A warrant for internal interception must specify the person or premises under consideration. That was sufficiently clear, from the perspective of the putative victim. "*Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA.*" (paragraph 160).

[4] Note the contrast between the finding in respect of mass interception (unlawful) in *Liberty* and the finding in respect of 'strategic interception' (inadmissible) in the earlier case of *Weber and Saravia v Germany* (Application No. 54934/00).

c. The provisions on duration, renewal and cancellation were sufficiently clear and comprehensive (paragraph 161);
d. The safeguards presented by the presence of the Information Commissioner and the IPT provide a sufficient level of scrutiny to UK surveillance activities (paragraphs 166-7).

40. The implications of both the *Liberty* and *Kennedy* cases are addressed in detail in the *Big Brother Watch* application which is currently pending before the ECtHR. We consider that the finding in *Kennedy* is, at least currently, determinative of the legality of the Section 8 (2) and (3) framework for internal communications. The ECtHR was not prepared to find a violation of Article 8. We consider that the judgment is not determinative for the purposes of scenario (a) because scenario (a) entails interception of bulk internal contents data contrary to RIPA.

41. Furthermore, *Kennedy* does not determine the position in respect of interception of external communications (section 8 (4)) or communications data. The ECtHR expressly relied on the fact that the provisions under challenge did not allow for the capture of large volumes of interception data. As set out above, RIPA does allow for that in respect of both external contents data and also in respect of communications data.

42. Accordingly, it is appropriate to ask whether the ECtHR would be likely to treat interception of external contents and of all communications data as more closely akin to that which it considered in *Liberty* (where it found a violation) or *Kennedy* (no violation).

43. In our view the RIPA provisions in respect of external content data and all communications data are clearly more closely analogous to the situation in *Liberty*. In particular, the Secretary of State has a wide discretion to determine what should be intercepted: she only has to describe the intercepted material and state that the interception is necessary. The outcome is very similar to that which the ECtHR considered in *Liberty*: mass interception of all material passing through submarine cables.

44. On the other hand, we note that the ECtHR has accepted (in *Kennedy*) that RIPA provides a satisfactory regime concerning the storage, retention and destruction of contents data.

45. Taking all of the factors into account, we conclude that the statutory framework in respect of the interception of external contents data is very probably unlawful. It provides too wide a discretion to the Secretary of State in respect of the categories and kinds of documents that can be retained. All that has to be identified is the kind of document in question. In theory, and perhaps in practice, the Secretary of State may order the interception of all material passing along a transatlantic cable. If that is the case, then RIPA provides almost no meaningful restraint on the exercise of executive discretion in respect of external communications.[5]

46. Turning to the position in respect of communication data (both internal and external), we note that RIPA is now 13 years old. As discussed above, the statute draws a sharp distinction between content and communications data. That distinction derives (at least to some extent) from the traditional 'postal' distinction between the address on the envelope and its contents. However, the significance of that boundary has been eroded by the realities modern internet usage. Communications data now encompasses each individual URL visited, the contents of an individual's Twitter and Facebook address lists, messages posted on social media websites and numerous other significant elements of an individual's online private life. Given modern trends in internet use, the binary distinction between contents and communications data has become increasingly artificial. Many of the most 'important' aspects of an individual's online 'private life' can be accessed via their communications data or 'metadata'.

47. RIPA requires only that the authorisation describes the communications data to be intercepted. Those authorisations can be 'signed off' by a wide variety of public bodies and persons. As a result, it allows for the mass interception of critical aspects of UK citizens' online 'private life'. Even with such safeguards and review mechanisms as RIPA provides, it offers insufficient clarity about the circumstances in which the executive may or may not authorise interception of communications data. In short, the rules concerning communications data are too uncertain and do not provide sufficient clarity to be 'in accordance with the law.'

48. As noted at paragraph 25 above, we have also considered briefly the possibility that GCHQ is intercepting data on the transatlantic cable so as to argue that it is outside of the jurisdiction and, therefore, not subject to RIPA at all. For the reasons set out in

[5] The IPT must have proceeded on the assumption that section 8(4) interception is lawful in case IPT/01/77. However, the issue does not appear to have been the subject of detailed consideration there, and in any event the case pre-dates the important ECtHR judgments in *Liberty* and *Kennedy*.

Liberty, we consider the mass interception of communications via a transatlantic cable to be unlawful, and that these conclusions would apply even if some or all of the interception is taking place outside UK territorial waters. In any event, we note that, during a debate on interception of data transferred via submarine cables that James Brokenshire (Parliamentary Under-Secretary of State for the Home Department) stated that GCHQ does not carry out interception outside of the scope of RIPA.[6]

49. In conclusion, in *Liberty* the ECtHR cited the mass interception of data, in the course of transmission via submarine cables, as one of the flaws of the pre-RIPA regime. We consider that the mass interception of external contents and communications data is unlawful for the reasons identified in *Liberty*. The indiscriminate interception of data, solely by reference to the request of the executive, is a disproportionate interference with the private life of the individuals concerned.

(B) RETENTION AND USE OF COMMUNICATIONS DATA

50. The Data Protection Act 1998 ('DPA') sets out a series of restrictions on the use to which 'personal data' may be put. However, section 28 of the Act provides:

> *"National security*
> *(1) Personal data are exempt from any of the provisions of -*
> *a. The data protection principles*
> *b. Parts II, III and V and*
> *c. Sections 54A and section 55*
>
> *If the exemption from that provision is required for the purpose of safeguarding national security.*
>
> *(2) Subject to subsection (4) a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions mentioned in subsection (1) is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact..."*

51. We have no information as to whether or not the Secretary of State has issued relevant section 28 notices. Nonetheless, what follows is based on the assumption that the Secretary of State may (and possibly has) taken some aspects of the intercept 'programme' outside of the scope of the DPA.
52. Section 15 of RIPA deals with the use of material acquired pursuant to an interception warrant (ie content data and possibly some related communications data). Subsection 2 requires that the data are not viewed by more persons than is necessary for the authorised purpose. Subsection 3 requires that, once the material

[6] HC Deb, 31 October 2013, c381WH.

is no longer necessary for its authorised purpose, it should be destroyed. Subsection 4 provides:

> "*(4) For the purposes of this section something is necessary for the authorised purposes if, and only if–*
>
> *(a) it continues to be, or is likely to become, necessary as mentioned in section 5(3);*
> *(b) it is necessary for facilitating the carrying out of any of the functions under this Chapter of the Secretary of State;*
> *(c) it is necessary for facilitating the carrying out of any functions in relation to this Part of the Interception of Communications Commissioner or of the Tribunal;*
> *(d) it is necessary to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution; or*
> *(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) RIPA itself places very few limits on the uses to which mass intercept data may be put.*"

53. Section 16 imposes some further safeguards for certified warrants under section 8 (4) (external communications):

> "*(1) For the purposes of section 15 the requirements of this section, in the case of a warrant in relation to which there is a section 8(4) certificate, are that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it–*
>
> *(a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and*
> *(b) falls within subsection (2).*
>
> *(2) Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which–*
>
> *(a) is referable to an individual who is known to be for the time being in the British Islands; and*
> *(b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him.*
>
> *(3) Intercepted material falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if–*
>
> *(a) it is certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in subsection 5(3)(a), (b) or (c); and*
> *(b) the material relates only to communications sent during a period specified in the certificate that is no longer than the permitted maximum.*
>
> *(3A) In subsection (3)(b) 'the permitted maximum' means–*
>
> *(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, six months; and*
> *(b) in any other case, three months.*
>
> *(4) Intercepted material also falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if–*
>
> *(a) the person to whom the warrant is addressed believes, on reasonable grounds, that the circumstances are such that the material would fall within that subsection; or*
> *(b) the conditions set out in subsection (5) below are satisfied in relation to the selection of the material.*
>
> *(5) Those conditions are satisfied in relation to the selection of intercepted material if–*

(a) it has appeared to the person to whom the warrant is addressed that there has been such a relevant change of circumstances as, but for subsection (4)(b), would prevent the intercepted material from falling within subsection (2);

(b) since it first so appeared, a written authorisation to read, look at or listen to the material has been given by a senior official; and

(c) the selection is made before the end of ***[*** *the permitted period* ***] 3*** *.*

(5A) In subsection (5)(c) 'the permitted period' means–

(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, the period ending with the end of the fifth working day after it first appeared as mentioned in subsection (5)(a) to the person to whom the warrant is addressed; and

(b) in any other case, the period ending with the end of the first working day after it first so appeared to that person.

(6) References in this section to its appearing that there has been a relevant change of circumstances are references to its appearing either–

(a) that the individual in question has entered the British Islands; or

(b) that a belief by the person to whom the warrant is addressed in the individual's presence outside the British Islands was in fact mistaken."

54. Section 23 sets out some of the limitations on the retention and use of 'communications data'. Thus they may not be disclosed to anyone other than the person who issued the notice or an individual specified in the notice (subsection 3). They may not be retained or disclosed beyond a period of one month (subsection 4). However, that month long period may be extended by a renewal application (subsection 7).

55. We are particularly asked whether data that have been intercepted may be submitted to 'pattern of life analysis.' We understand that pattern of life analysis involves the gathering together of a large body of data about a particular individual. In this context it ordinarily refers to communications data: who does the individual communicate with, which websites do they visit, what are their associations and interests? However, it could refer to contents data as well: what do they say to their associates?

56. RIPA does not place any restrictions on the uses to which intercept material might be put (other than its admissibility in court). Therefore all three categories of data (internal contents data; external contents data and communications data) may in principle be subjected to pattern of life analysis, as long as those data are lawfully held. We address below the implications of the Article 8 case law on the legality of this statutory regime.

57. RIPA also places no express restriction on members of the Security Services retaining and analysing data of 'non-suspects'. Where contents data are obtained in

relation to a particular subject it may be unlikely, but remains possible, that the person is a non-suspect. In respect of external data, the only restriction (under section s 8 (4) and 22 (3)) is that those data must have fallen within the description of data to be intercepted. For example, they must have contained a particular keyword, used a particular server or been directed to a particular individual or group of individuals. Once the data are lawfully within the possession of GCHQ, RIPA contains no restrictions on their use.

Is the statutory framework lawful?

58. The Article 8 case law has provided a clear line of authority concerning the use to which intercept material may be put. In *Liberty* the ECtHR criticised the lack of restrictions placed on the uses to which intercepted data might be put under the pre-RIPA regime. In *Kennedy* the Court found that:

> "*As regards the procedure for examining, using and storing the data, the Government indicated in its submissions that, under RIPA, an intercepting agency could, in principle, listen to all intercept material collected. The Court recalls its conclusion in Liberty at [65] that the authorities' discretion to capture and listen to captured material was very wide. However, that case, unlike the present case, involved external communications, in respect of which data were captured indiscriminately. Contrary to the practice under the Interception of Communications Act 1985 concerning external communications, interception warrants for internal communications under RIPA relate to one person or one set of premises only, thereby limiting the scope of the authorities' discretion to intercept and listen to private communications. Moreover, any captured data which are not necessary for any of the authorised purposes must be destroyed.*"

59. RIPA imposes a fuller and clearer framework for the retention, viewing and destruction of intercepted content data than that which applied previously. In particular, it restricts the number of persons that might view any intercepted material and requires that the number of copies made must be no more than the minimum necessary (section 15 (2)). The material must also be destroyed when there are no longer any grounds for retaining it (15 (3)).

60. However, it is clear from the quotation set out above that the ECtHR's conclusions in *Kennedy* were influenced (at least in part) by the fact that the data in question were targeted and limited in scope: they were internal contents data. The restrictions on use and retention provide sufficient protection in those circumstances.

61. In our view the position in respect of mass data (external contents data or communications data) is different. We consider it well arguable that where large volumes of data are being retained, including the data of 'non-suspects', there should

be more stringent safeguards concerning the uses and destruction of those data. The arguments are relatively finely balanced,[7] but in our view a court would probably hold that the restrictions on retention, storage and reproduction of external contents data and communications data are insufficiently robust, and that the UK is therefore in violation of its Article 8 obligations.

(C) DATA SHARING

62. Under scenario (c) we are asked whether it is lawful for intercepted data to be transferred to the security services of another foreign power, for example the NSA.

63. RIPA only provides a 'light touch' framework for the transfer of data to third party powers. Section 15 (2) and (3) restrict the number of persons (within the UK) who may view intercepted contents data (and related communications data) and require that the data are destroyed when there are no longer any grounds for retaining them. However, subsection (6) removes those restrictions where the data are to be transferred overseas:

> *"Arrangements in relation to interception warrants which are made for the purposes of subsection (1) -*
>
> *(a) Shall not be required to secure that the requirements of subsections (2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom; ..."*

64. The only restriction on the use of such data transferred overseas is provided by section 15(7):

> *"The requirements of this subsection are satisfied in the case of a warrant if it appears to the Secretary of State –*
>
> *(a) That requirements corresponding to those of subsection (2) and (3) will apply, to such extent (if any) as the Secretary of State thinks fit, in relation to any of the intercepted material or related communications data possession of which or of any copy of which is surrendered to the authorities in question..."*

65. Furthermore, the Secretary of State must determine that there are mechanisms in place in the receiver state to prevent a disclosure in court, contrary to section 17.

66. As a result, the Secretary of State has an extremely wide discretion to determine whether or not the requirements of subsections (2) and (3) need apply at all. There

[7] In particular, we note that the contrary argument receives some support from the Decision of the IPT in IPT/01/77. However, that Decision pre-dates the judgments in both *Liberty* and *Kennedy*, and can be distinguished for that reason.

are no restrictions on the transfer of data obtained under an interception warrant beyond those that the Secretary of State considers necessary.

67. The position in respect of communications data is again materially different. RIPA makes no express reference to transfer of such data. Section 15 is said to apply only to interception 'warrants' (ie it does not apply to data obtained under an authorisation). The consequence might either be that there are no restrictions on transfer or that no transfer to other governments is authorised at all.

68. We consider that the better view is that RIPA does not authorise transfer of communications data to other governments. RIPA makes provision for transfer of data obtained pursuant to warrants. It also sets out which individuals may receive (via disclosure) material obtained pursuant to a section 22 and 23 authorisation/notice. Therefore, the best reading of the statute is that it does not allow for the transfer of communications data obtained under an authorisation.

69. Scenario (c) proceeds on the basis that the UK government may share communications data, obtained via interception, with other governments (in particular the US government). The only conceivable basis on which such a transfer could be lawful if it is not sanctioned by RIPA is that it is conducted pursuant to the Crown's common law powers. Whilst it is well-established that the Crown has such powers (unlike statutory public bodies who may also collect communications data under authorisations),[8] we seriously question the propriety of the government relying on non-statutory (and hence necessarily unwritten and uncertain) powers in this field.

Is the statutory framework lawful?

70. When data are transferred to another authority, that constitutes a fresh interference with an individual's Article 8 rights. That interference must be assessed on a free-standing basis (*Weber v Germany* (Application No. 54934/00) para 79)).

71. There are powerful reasons why security services in different states should be able to co-operate with one another. Many of the threats addressed by the security services are trans-national in nature. Given that some intercept data may be lawfully obtained

[8] On the relationship between prerogative and statutory powers see the speeches of Lords Hoffman and Bingham in *R (Bancoult) v Secretary of State for Foreign and Commonwealth Affairs (No 2)* [2008] UKHL 61.

and transferred, it is reasonable to ask what safeguards might be put in place to protect the right to privacy of the individuals concerned? Those safeguards might be set out in either a Memorandum of Understanding ('MoU') or a bilateral agreement between the UK and US governments.

72. RIPA itself envisages that the UK government may enter into MoUs that relate to the provision of mutual assistance in this area. All requests for assistance, where such agreements exist, must be made with lawful authority (section 1 (4)).

73. In principle the government could either:
    a. Insist that data transferred is held, used and destroyed by a foreign government to the same standards and on the same basis that it is held by the UK government; or
    b. Enter into an MoU or other agreement that imposes appropriate restrictions on the use, retention and destruction of the data; or
    c. Leave the question of data use to the unfettered discretion of the Secretary of State; or
    d. Impose no restrictions on transfers to other security services whatsoever.

74. RIPA adopts the third option. We consider that such an approach is not sufficient for at least three reasons. First, the transfer of private data is a significant interference with an individual's Article 8 rights. That interference will only be lawful when proportionate. One aspect of that proportionality assessment must include the retention and use of the data once transferred. Secondly, the ECtHR has held on more than one occasion that surveillance, and the use of surveillance data, is an area in which governments must conduct themselves in a transparent and 'predictable' manner. The current framework is uncertain: it relies on the discretion of one individual.

75. Thirdly, on a pragmatic level, given the degree of data transfer between international security services, there is a real possibility that the NSA might function as GCHQ's unofficial 'backup' service. If GCHQ is not entitled to hold onto data itself, it might transfer it to the NSA. In time, and if relevant, that data might be transferred back to GCHQ. Without strong guidelines and scrutiny, the two services might support each other to (in effect) circumvent the requirements of their domestic legislation. We are aware that the framework governing the gathering and storage of data by the NSA is currently under review and that President Obama has recently announced certain

reforms. Once those reforms are fully developed, it may be necessary to revisit this aspect of our Advice.

76. Therefore, we consider that RIPA probably allows the unfettered transfer of data to the NSA, checked only by the views of the executive. That is not 'in accordance with the law', and is therefore contrary to Article 8 and unlawful.

77. We also consider that, if GCHQ transfers communications data to other governments it does so without any statutory restrictions. Such transfers are a disproportionate interference with the Article 8 rights of the individuals concerned. There are no restrictions, checks or restraints on the transfer of that data.

78. If there was a published UK-US MoU or agreement governing the transfer, use and destruction of data by the NSA, that might go some way towards resolving some of our concerns. The use of MoUs to address human rights concerns is controversial, and any proposal would need to be given detailed further consideration. Nonetheless, we recognise that MoUs have received some degree of sanction from the ECtHR in some cases,[9] and might represent an achievable way forward in relation to these issues.

(D) USE OF INTERCEPT DATA TO CARRY OUT DRONE STRIKES

79. Under scenario (d), we are asked whether mass intercept data may be lawfully transferred to another state that uses it for the purpose of carrying out a drone strike conducted outside of a conventional conflict scenario.

80. There have been a number of Convention cases in recent years that have touched on this question of principle. In *Chahal v United Kingdom* (Application no. 22414/93), the ECtHR held that an individual could not lawfully be deported to a country where they face a real risk of torture. The UK government cannot disavow responsibility for the consequences of handing over an individual to a foreign state.

81. However, in *Abu Qatada v United Kingdom* (Application no. 8139/09), the UK government had entered into an MoU with Jordan, which provided that the individual concerned would not be tortured on his return to Jordan. The ECtHR concluded that

[9] *Abu Qatada v United Kingdom* (Application no. 8139/09).

Abu Qatada could be deported because the MoU was sufficiently robust to secure his protection.

82. We are conscious that the argument might be advanced that the United Kingdom government does not owe any Convention duties to individual victims of drone strikes in third states (*Al-Skeini v United Kingdom* (Application no. 55721/07). Furthermore, there are obvious distinctions between transferring an individual who will be subject to torture and transferring data that might be used in order to kill. Therefore, it is certainly arguable that the Convention case law has no application in this context.

83. However, we are of the opinion that, even if the Convention case law does not apply, the transfer of data to facilitate a drone strike is likely to be unlawful for the purposes of English law because the drone strike itself would not be a lawful act, if carried out by the UK government. Therefore anyone who transfers data to facilitate that strike will be an accessory to an unlawful act, for the purposes of English law.

84. The lawfulness, or otherwise, of data transfer for drone strikes was recently addressed in the case of *R (Khan) v Secretary of State for the Foreign and Commonwealth Office* [2014] EWCA Civ 24. The claim was brought by the son of a man killed by a drone strike in Pakistan. He asserted that:
    a. The drone strike was carried out by the US government;
    b. The drone strike had been initiated using 'locational intelligence' provided to the CIA by GCHQ;
    c. Preventative drone strikes against non-combatants are unlawful, for the purposes of English law;
    d. Therefore, GCHQ employees providing locational intelligence, that they knew would be used for the purpose of drone strikes, are at risk of prosecution as secondary parties to murder.

85. The court at first instance refused permission for the judicial review on the grounds that it would not make a declaration as to the lawfulness of the acts of a foreign state. The court made no finding as to the lawfulness or otherwise of data transfers by GCHQ staff. The Court of Appeal upheld that decision on 20 January 2014. Permission was refused on justiciability grounds, but the court did not express a view on the lawfulness of data transfers in support of a drone strike (paras 16 and 19). We are mindful of the consequences of the Court of Appeal's decision, but consider that

it does not preclude us from expressing a view on the substantive question of the legality of the act of transfer.

86. Individuals participating in war are entitled to kill one another; they can invoke the defence of 'combatant immunity'. Both domestic and international law recognise the status of some individuals as 'lawful combatants' engaged in 'international armed conflict'. Killing an individual outside of that framework is murder. Assisting in the killing of an individual outside of that framework is assisting in the act of murder.[10]

87. In our view, the drone strikes carried out by the CIA in Yemen and Pakistan (amongst other places) are not carried out in the context of an 'international armed conflict'. The US is not at war with Yemen or Pakistan. The individuals who are targeted are not, therefore, 'combatants' and their killers are not entitled to 'combatant immunity'.

88. The US Government has sought to justify the attacks by reference to the doctrine of 'anticipatory self-defence'. Article 51 of the UN Charter provides:

> *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."*

89. Proponents of anticipatory self-defence argue that the individuals targeted are a threat to US interests: they have been or are involved in planning attacks against targets on the US mainland or overseas. The individuals who are targets of the drone strikes are not engaged in a conventional war against US forces. Nonetheless, they are combatants in a wider sense. Therefore, it is argued that an attack on those individuals is an act of self-defence, even though the individuals themselves do not (at the moment the strike is made) represent an imminent threat to US interests.[11]

90. Furthermore, they rely on the fact that (at least in some cases) the strikes have been carried out with the consent of the Yemeni and Pakistani authorities.

---

[10] Ministry of Defence, *Manual of the Law of Armed Conflict* (OUP, 2004), p. 37.
[11] See the US Department of Justice Paper, '*Lawfulness of a Lethal Operation Directed against a US Citizen who is a Senior Operational Leader of Al-Qa'ida or an Associated Force*' DOJ White Paper 020413.

91. The doctrine of anticipatory self-defence, as argued by the US government, has not been widely accepted within international law. The doctrine of anticipatory self-defence provides that, where the target presents an 'imminent' or 'immediate' threat, a state may strike first in self-defence. In effect, the attacking party must strike or be struck. The US government relies on a broader formulation of that principle. They cannot know, or demonstrate, that the targets of any particular drone strike present an imminent threat to US interests. In effect, they rely on intelligence and other information to argue that the targets might present an imminent threat. That broader formulation of the doctrine has not yet become a part of the consensus of international law. Indeed, to the contrary, it was the rationale advanced by Israel in order to justify a pre-emptive bombing strike on an Iraqi nuclear reactor over 30 years ago. That justification was rejected by the Security Council.[12]

92. The UK government has also rejected this formulation of the doctrine of anticipatory self defence much more recently. In his written report to Prime Minister Tony Blair, when evaluating the lawfulness of the invasion of Iraq, the Attorney General wrote:

> *"... I am aware that the USA has been arguing for recognition of a broad doctrine of a right to use force to pre-empt danger in the future. If this means more than a right to respond proportionately to an imminent attack (and I understand that the doctrine is intended to carry that connotation) this is not a doctrine which, in my opinion, exists or is recognized in international law."*

93. Therefore, we consider that the doctrine of anticipatory self-defence does not provide a sound legal basis for targeted assassinations, via drone strikes, in United Kingdom law.[13] We are aware of the recent report concerning drone strikes by Ben Emmerson, the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. We agree with his conclusion that there needs to be an international dialogue concerning the scope of anticipatory self-defence and the definition of combatant immunity (see paragraphs 79ff).[14] However, in our opinion, current domestic (and international) law has not embraced the broader version of anticipatory self-defence. The United Kingdom government does not and could not lawfully carry out drone strikes outside Afghanistan, such as those carried out by the US government in Yemen and Pakistan. Accordingly, in our view, if GCHQ transferred data to the NSA in the knowledge that it would or might be used for targeting drone strikes, that transfer is

---

[12] Security Council Resolution 487 (19.06.81).
[13] Whether or not the strikes are lawful, for the purposes of international law is a connected, but not identical question.
[14] http://www.lawfareblog.com/wp-content/uploads/2013/10/Emmerson-Report.pdf

probably unlawful. The transferor would be an accessory to murder for the purposes of domestic law.

94. We are further asked about the precise scope of the obligations owed by the UK government where it knows or suspects that information which it is disclosing might be used for an unlawful purpose. We consider that pre-existing case law does not provide a precisely analogous set of facts.

95. If the victims of the unlawful act were in the United Kingdom, the UK government would have an obligation to investigate. The ECtHR has repeatedly held that a procedural obligation to investigate arises where credible allegations are made that an individual's right to life has been breached (*Edwards v. The United Kingdom*, Application no. 46477/99 (para. 69); *Varnava and Others v. Turkey*, (Application no. 16064/90 para 191). However, the victims of the unlawful acts are in a third state and are not under the 'effective control' of the UK government (*Al-Skeini v United Kingdom* Application no.55721/07). Arguably, therefore, the UK government does not owe them any ECHR obligations to investigate.

96. Furthermore, if the UK government was seeking to rely on evidence in court, that might have been obtained unlawfully, it would be obliged to carry out an investigation into the origins of that information. In *A and others v Secretary of State for the Home Department* [2005] UKHL 72 the House of Lords was divided over the obligations that should arise where a defendant to proceedings before SIAC raises a credible argument that information used against them may have been obtained via torture. The majority held that, the Court must carry out an investigation and satisfy itself (on the balance of probabilities) that it was not.[15] We are aware that the analogy is by no means a perfect one. The principle laid down in *A* is a rule of admissibility: it does not govern the carrying out of anti-terror operations.

97. In *Re McKerr* [2004] UKHL 12, the House of Lords held that there was no freestanding common law obligation to carry out an Article 2 compliant investigation, where a death occurred before the passage of the Human Rights Act.[16] Parliament has legislated to delineate the scope of the duty to investigate death. Therefore, the common law will not impose additional obligations beyond that duty. However, Lord

[15] There were powerful speeches by the minority (including Lord Bingham's lengthy speech) which imposed a higher threshold.
[16] See the moderation of that position in *In the matter of an application by Brigid McCaughey and another for Judicial Review (Northern Ireland)* [2011] UKSC 20.

Steyn *obiter dicta* also suggested that the principles of customary international law might still impose an obligation on the United Kingdom to investigate, in cases where a death did not attract the protection of the ECHR (paras 52-3). Customary international law, in his argument, forms part of the common law of England and, therefore, the question could be justiciable in England. Even if it does not, by failing to carry out an investigation the UK government would be in breach of customary international law. Needless to say, it would be necessary to demonstrate a sufficient nexus between an act of the UK government and the death in question.

98. A separate, but related, principle was articulated by the majority of the ECtHR in *Silih v Slovenia* (Application No. 71463/01). The case concerned the death of an individual who had been killed before the ECHR came into effect. The Court held that, where the investigation of the death takes place after the Convention has come into force, it must be compliant with Article 2. The majority also held that:

> *"163 Secondly, there must exist a genuine connection between the death and the entry into force of the Convention in respect of the respondent State for the procedural obligations imposed by art.2 to come into effect.*
> *Thus a significant proportion of the procedural steps required by this provision—which include not only an effective investigation into the death of the person concerned but also the institution of appropriate proceedings for the purpose of determining the cause of the death and holding those responsible to account —will have been or ought to have been carried out after the critical date.*
> ***However, the Court would not exclude that in certain circumstances the connection could also be based on the need to ensure that the guarantees and the underlying values of the Convention are protected in a real and effective manner."*** *(emphasis added)*

99. The finding in *Silih* was criticised by the Supreme Court in *McCaughey*, particularly in Lord Roger's dissenting judgment. Nonetheless, they followed it. We are aware that *Silih* was concerned with temporal questions of justiciability. However, we consider that the same principle will arguably apply to spatial questions of justiciability (the deaths have occurred in Pakistan or Yemen). Unfortunately the various judgments in *McCaughey* did not revisit Lord Steyn's *dicta*. We consider that both the *dicta* of Lord Steyn and the views of the ECtHR in *Silih* are relevant to the scenario set out in our instructions. On the facts before us, the UK government knows, or suspects that: (a) a transfer of data is being made on its territory and (b) that transfer is being carried out or aided by agents of the UK government. We consider that, pursuant to the transfer, the agent is likely to become an accessory to murder. On those facts it is certainly arguable that the government is obliged, pursuant to customary international law, to take reasonable steps to investigate the transfer and prevent that unlawful

act. Alternatively, the ECtHR has held that the obligation to investigate can arise where it is necessary to protect the underlying values of the ECHR. It is difficult to imagine a set of circumstances that would be more likely to trigger that requirement.

100. Furthermore, in *R v Registrar General (ex parte Smith)* [1991] 2 Q.B. 393, the Court of Appeal held that Parliamentary legislation should be interpreted in a manner that did not enable a person to commit or to escape liability for a crime resulting in a danger to life (affirmed by the Supreme Court in *Welwyn Hatfield Council v Secretary of State for Communities and Local Government* [2011] UKSC 15). They held that public policy would not allow for any other outcome. Being an accessory to murder is a crime resulting in a danger to life. Therefore, we consider that, in order for the principle in *Smith* to be effective, the statutory framework concerned with the investigation of death should apply to cases of this kind. If there is no current obligation to investigate deaths of this kind, public policy arguably demands that there should be. State employees should not be entitled to rely on the gaps in the current statutory framework to commit serious crime with impunity. The main obstacle in the way of this argument would be the justiciability issues confronted in *Kahn* and addressed at paras [84-5] above. A version of this submission formed the basis of the claimant's secondary case, which the Court of Appeal considered was non-justiciable as impugning the US for the same reasons as they accepted in relation to the primary case. However, even if the courts would not be prepared to apply the *Smith* principle directly, in our view it would be surprising (and undesirable) if the UK government were able to rely on justiciability arguments so as to evade any obligation to investigate cases where state employees have potentially become accessories to murder. Such a result, even if non-justiciable, would be contrary to the requirements of good governance and public policy.

101. The precise scope of the duty to investigate which would arise is the subject of legitimate debate. It might be said that the investigation does not need to meet the 'high' threshold imposed by the Article 2 case law. However, we consider that, given the seriousness of the issues in question, there is no reason why it should not have to do so. Indeed, if the duty derives from the ECHR or customary international law, it should. That investigation should inform the contents of any subsequent 'prevention' policy.

102. The most obvious mechanism by which the obligation to prevent could be implemented is via an MoU or other bilateral agreement concerning the uses to which transferred data might be put. It is impractical to suggest that the government should obtain undertakings or carry out investigations in respect of each piece of data transferred. We understand that no such MoU or other agreement exists. Absent an agreement, and assuming that the data transferred might be used to target drone strikes, we consider that their transfer is on balance likely to be unlawful.

(E) DATA HUBS ON UK SOIL

103. Under scenario (e) we have been provided with two possible situations. Firstly a UK base (operated under the 1951 NATO Status of Forces Agreement) is used to transfer data to America. Some of those data have been obtained overseas by unlawful means. Secondly a UK base is used to transfer data from the mainland USA to bases overseas. Those data, instructions and orders are used to facilitate and carry out drone strikes.

104. The 1951 NATO Status of Forces Agreement provides:

> *"Article II*
>
> *It is the duty of a force and its civilian component and the members thereof as well as their dependents to respect the law of the receiving State, and to abstain from any activity inconsistent with the spirit of the present Agreement, and, in particular, from any political activity in the receiving State. It is also the duty of the sending State to take necessary of measures to that end.*
>
> ...
>
> *Article VII*
>
> 1. *Subject to the provisions of this Article,*
>   a. *the military authorities of the sending State shall have the right to exercise within the receiving State all criminal and disciplinary jurisdiction conferred on them by the law of the sending State over all persons subject to the military law of that State;*
>   b. *the authorities of the receiving State shall have jurisdiction over the members of a force or civilian component and their dependents with respect to offences committed within the territory of the receiving State and punishable by the law of that State.*
> 2.
>   a. *The military authorities of the sending State shall have the right to exercise exclusive jurisdiction over persons subject to the military law of that State with respect to offences, including offences relating to its security, punishable by the law of the sending State, but not by the law of the receiving State.*
>   b. *The authorities of the receiving State shall have the right to exercise exclusive jurisdiction over members of a force or civilian component and their dependents with respect to offences, including offences relating to the security of that State, punishable by its law but not by the law of the sending state.*

c. *For the purposes of this paragraph and of paragraph 3 of this Article a security offence against a State shall include:*
   i. *treason against the State;*
   ii. *sabotage, espionage or violation of any law relating to official secrets of that State, or secrets relating to the national defence of that State*

3. *In case where the right to exercise jurisdiction is concurrent the following rules shall apply:*
   a. *The military authorities of the sending State shall have the primary right to exercise jurisdiction over a member of a force or of a civilian component in relation to*
      i. *offences solely against the property or security of that State, or offences solely against the person or property of another member of the force or civilian component of that State or of a dependent;*
      ii. *offences arising out of any act or omission done in the performance of official duty.*
   b. *In the case of any other offence the authorities of the receiving State shall have the primary right to exercise jurisdiction.*
   c. *If the State having the primary right decides not to exercise jurisdiction, it shall notify the authorities of the other State as soon as practicable. The authorities of the State having the primary right shall give sympathetic consideration to a request from the authorities of the other State for a waiver of its right in cases where that other state considers such waiver to be of particular importance.*

...

6. *The authorities of the receiving and sending States shall assist each other in the carrying out of all necessary investigations into offences, and in the collection and production of evidence, including the seizure and, in proper cases, the handing over of objects connected with an offence. The handing over of such objects may, however, be made subject to their return within the time specified by the authority delivering them.*"

105. It is clear from the Agreement that NATO servicemen, on operations overseas, must act in line with the law of the receiving state (here, UK law). Pursuant to Article VII, the UK government has exclusive jurisdiction in relation to breaches of UK law that are not also breaches of US military law.

106. We turn now to the first situation envisaged under scenario (e). The simplest set of facts concerns the transfer, via UK soil, of data that have been obtained in breach of international law. For the purpose of what follows we assume that US servicemen in the UK play an active part in the transfer of those data.

107. We are not aware of any authorities that deal directly with this point. There are two possible analogies which might assist. First, if the United States forces were transferring illegal physical goods (such as contraband) via UK soil, that would be a breach of the Forces Agreement. Article XI (and elsewhere) requires NATO forces to obey the customs laws of the receiving country (with some exceptions).

108. A second possible analogy arises out of the case of *El-Masri v Former Yugoslavian Republic of Macedonia* (Application no.39630/09). The ECtHR held that the Republic of Macedonia had breached the Article 3 rights of a German citizen whom they had detained and then transferred to the CIA for on-transfer to Afghanistan. He was interrogated and tortured there. The Court's decision relied on the Macedonian government's knowledge of the destination of the flight they put him on, the lack of a CIA warrant for his arrest and the Macedonian government's knowledge of the rendition process from publicly available information at the time (paras 215-22).

109. We consider that the findings in *El-Masri* do not easily map onto the facts in this case. The Macedonian government knew, in effect, that the transfer of Mr El-Masri was a transfer to torture. Here, the UK government has stated that it does not know what support to US operations is being provided from RAF Croughton [HC Deb, 25 March 2013, c939W]. Furthermore, in *El-Masri* there was a specific individual whose Article 3 rights had been violated.

110. In our view, the contraband/trafficking analogy provides a clearer and more useful comparator. If the US government was shipping unlawful goods via the UK (via a NATO base), and the UK government was aware of that fact, then the US forces would be in breach of the Agreement. The UK government would have the right to object and ultimately to press charges.

111. Applying those principles to the transfer of drone strike data and orders, the outcome is similar. The UK government is entitled to object, and ultimately to bring a prosecution, where visiting forces break English law. However, they have no obligation to do so under the Forces Agreement: they 'may' do so. Ultimately the responsibility to press charges against US servicemen lies with the Director of Public Prosecutions (if they consider that it is in the public interest to do so). Alternatively, the UK government might object that the transfer is in breach of any MoU between the two states, assuming that such an MoU exists.

112. However, we are aware that a prosecution of that kind is extremely unlikely to occur. In particular we note that the UK government does not appear to know what takes place, with any degree of detail, on those bases. It appears that an RAF liaison officer is assigned to each base (HC Deb, 25 March 2013, c939-940W). However, the scope of their duties and powers to review or investigate, if any, are unclear. We

note that none are set out in the Visiting Forces Act, and there is no obligation to monitor compliance with UK law or indeed report on the activities of NATO partners at the bases. As noted above, in answer to a Parliamentary Question, in March 2013, the Minister of State for the Ministry of Defence (Andrew Robathan) could not tell Parliament whether or not the US forces were undertaking activities in connection with the US drone programme from RAF Croughton (HC Deb, 25 March 2013, c939-940W).

113. In practical terms, we consider it unlikely that the UK government will have any knowledge of what data is passing through UK communications hubs on a day to day basis. Therefore, even though they have a power to prosecute, that power is highly unlikely to be exercised. Furthermore, whilst it is possible to bring a judicial review to challenge a decision of the DPP not to prosecute, such a claim would be very unlikely to succeed (see *R v DPP* [2001] QB 330 per Bingham CJ at 343 ff).

114. We are instructed that consideration is currently being given to amendments to the Visiting Forces Act (1952) and RIPA which would introduce basic reporting requirements on RAF Commanders and a new scrutiny group present on US bases and/or the Information Commissioner. In our view, and pending review of the existing legislative framework, such amendments might go some way to ensuring that Ministers are informed about data passing through the UK. This, in turn, would assist the government to monitor compliance with UK law and make informed decisions about whether there is a need for an MoU or other multilateral agreement between NATO partners.

JEMIMA STRATFORD QC

TIM JOHNSTON

Brick Court Chambers

22 January 2014