SUBMISSION TO THE HOME OFFICE'S CONSULTATION ON THE INTERCEPTION OF COMMUNICATIONS CODE OF PRACTICE FROM THE APPG ON DRONES

INTRODUCTION

1. This submission is concerned with the Home Office's proposed amendments to the existing Interception of Communications Code of Practice ('the Code'). The Officers of the All Party Parliamentary Group on Drones ('the APPG') welcome the opportunity to provide input into the Code on behalf of the APPG. The APPG has a particular interest in the interception of communications as a preliminary step in the gathering and use of intelligence to facilitate lethal drone strikes, and the legal and human rights implications thereof.

2. The APPG notes the publication during the consultation period of a major report by the Intelligence and Security Committee of Parliament ('the ISC Report').[1] The ISC Report recommends that the current statutory framework – including the Regulation of Investigatory Powers Act 2000 ('RIPA') – be repealed and overhauled by one single, comprehensive statute setting out clearly the powers of the intelligence and security agencies and the safeguards on the exercise of those powers. Clearly if this course of action were to be pursued the Code might become redundant. However, it is likely that many of the issues raised in the course of this consultation would ultimately require attention in the drafting of a new bill: this makes the consultation a useful exercise in any event.

BACKGROUND

3. In January 2014 the APPG Chair, Tom Watson MP, sought independent advice from barristers Jemima Stratford QC and Tim Johnston on the lawfulness of five assumed scenarios concerning the interception of communications. The advice set out five key conclusions:

[1] '*Privacy and Security: A Modern And Transparent Legal Framework*', March 2015, available at http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf.

a. The bulk interception of external communications – *i.e.* communications sent or received outside the British Islands – was lawful under RIPA but likely to amount to a disproportionate interference with the privacy rights of those affected under Article 8 of the European Convention on Human Rights ('the ECHR').

b. The statutory safeguards with regard to the retention, use and destruction of communications data (also known as metadata) and external communications were insufficiently stringent, and also likely to violate Article 8 ECHR.

c. The Secretary of State had a wide and largely unrestrained discretion to permit the transfer of intercepted communications to foreign powers. This unfettered discretion was incompatible with the requirements of the ECHR.

d. The transfer of data to foreign powers, in the knowledge that they were likely to be used to facilitate drone strikes against non-combatants, was probably unlawful and could, at least in theory, give rise to criminal liability on the part of those individuals involved.

4. A copy of the advice is attached as Annex 1.[2] The advice has previously been submitted on behalf of the APPG to the Intelligence and Security Committee ('ISC') and the Royal United Services Institute, and was referred to in the APPG's responses to two prior consultations – the Home Office's consultation on the Covert Surveillance Code of Practice[3] and the Information Commissioner's Office's consultation on the CCTV Code of Practice.[4]

[2] Also available at: http://appgdrones.org.uk/wp-content/uploads/2014/08/APPG_Final_advice.pdf. The scenarios, whilst assumed for the purposes of the advice, were based on news reports of the Edward Snowden leaks.

[3] http://appgdrones.org.uk/wp-content/uploads/2014/08/SUBMISSION-TO-THE-HOME-OFFICEfinal262.pdf

[4] http://appgdrones.org.uk/wp-content/uploads/2014/08/SUBMISSION-TO-THE-ICO-FINAL-26-6-2-3.pdf

5. In addition, following correspondence with Professor Sir David Omand, the authors of the advice prepared a supplementary note, attached as Annex 2.[5]

6. The Home Office will also be aware of the important judgments of the Investigatory Powers Tribunal ('IPT') in the actions brought by Liberty, Privacy International *et. al.*, which were published on 5 December 2014 and 6 February 2015. Those judgments held that the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, obtained by US authorities, contravened Articles 8 or 10 ECHR, but that following disclosures made in the course of the hearings themselves the violations had come to an end.

7. Finally, the APPG notes that two of its officers, Chair Tom Watson MP and Vice-Chair David Davis MP, have brought proceedings against the Home Secretary seeking a declaration that section 1 of the Data Retention and Investigatory Powers Act 2014 ('DRIP') is incompatible with Article 8 ECHR and Articles 7 and 8 of the European Union Charter of Fundamental Rights, in the light of the decision of the Court of Justice of the European Union in the *Digital Rights Ireland* case.[6] Mr. Watson and Mr. Davis have brought this action in their individual capacities as Members of Parliament, not on behalf of the APPG. However, in light of the ongoing proceedings, this submission will not address any amendments to the Code arising from DRIP.[7]

8. The issue of interception of communications has given rise to concerns amongst many Members of Parliament over the last year, as well as amongst the leading human rights NGOs, including Liberty, Privacy International, Big Brother Watch, Open Rights Group and Reprieve.[8] An Early Day Motion on the subject of state surveillance, tabled by Mr. Watson MP in June 2014, was signed by 43 Members of Parliament.[9]

---

[5] The APPG is grateful to Professor Sir David Omand for agreeing to disclosure of this note.
[6] Joined Cases C-293/12 and C-594/12.
[7] For the avoidance of doubt, this submission is made by the Officers in their capacity as Officers of the APPG, on behalf of the APPG and without prejudice to any evidence or submissions made in Mr. Watson and Mr. Davis's claim against the Home Secretary.
[8] See Liberty brief to Independent Reviewer of Terrorism Legislation
[9] Available at: http://www.parliament.uk/edm/2014-15/147.

LIMITS TO CONSULTATION

9. As a preliminary matter, the APPG notes that the Home Office does not seem to have made available a version of the new Code that 'tracks' or otherwise shows clearly the changes made to the previous draft. The unintended consequence may be that small but potentially significant changes to the Code pass unnoticed. For example, para 4.6 of the previous version of the Code – which deals with urgent authorisation of section 8(1) warrant – states that "*an urgent case is one in which interception authorisation is required within a twenty four hour period*". The equivalent para 5.6 of the new Code omits that sentence, with the result that the concept of an "*urgent*" case does not appear to be defined in the new Code. As the ISC Report highlights, transparency concerning the limits and safeguards that apply to the intrusive powers given to security and intelligence agencies is essential. In the interests of transparency, the APPG suggests that in future all proposed changes to those safeguards be identified as clearly as possible.

10. In a broad sense, the focus of the Code is on clarification of the statutory safeguards already in place rather than substantive improvement of those safeguards. In other words, the consultation exercise proceeds on the basis that the overarching regulatory framework is lawful and adequate. It is not clear that this is true. Public consultations, required under existing statutory provisions, are no substitute for a comprehensive review of RIPA and the six other Acts of Parliament that apply to intrusive capabilities: the Security Service Act 1989; the Intelligence Services Act 1992, the Wireless Telegraphy Act 2006; the Telecommunications Act 1984; the Counter-Terrorism Act 2008; and DRIP.

THE DRONES CONTEXT

11. The APPG's primary concern with the Code is its failure to consider (or consider adequately) the sharing and end-use of intercepted data by a foreign state.

12. As summarised by Jemima Stratford QC and Tim Johnston, the current position under RIPA is as follows:

    a. Subsections 15(2) and 15(3) of RIPA limit the number of persons to whom intercepted communications (and related metadata) may be disclosed, and the extent to which the data are disclosed, to the minimum necessary for the authorised purposes.

    b. However, subsection 15(6) lifts those requirements in relation to communications and metadata shared with foreign countries.

    c. In respect of data transferred overseas, the Secretary of State has a wide discretion to decide whether requirements corresponding to those in subsections 15(2) and 15(3) need apply and, if so, to what extent.

    d. The Secretary of State also has discretion to decide whether restrictions need be in place to prevent the disclosure of the intercepted material in a foreign court and, if so, to what extent.

13. As the supplementary note by Ms. Stratford and Mr. Johnston clarifies, the Intelligence Services Act 1994 also provides (at section 4) that the Director of GCHQ must ensure that GCHQ does not disclose any information except so far as necessary for the proper discharge of its functions (or for the purpose of criminal proceedings). Section 2 imposes a similar duty on the Chief of the Intelligence Service. Section 2 of the Security Service Act 1989 imposes substantially the same obligation on the Director-General of the Security Service.

14. Finally, Ms. Stratford and Mr. Johnston point out that section 15 of RIPA is only expressed to apply to data (and related metadata) acquired under warrants. RIPA sets out a different scheme for the interception of pure metadata; this does not require a warrant, merely an 'authorisation' (section 22). There is an ambiguity in RIPA as to whether the disclosure of metadata obtained under an authorisation to a foreign power is

allowed at all; but if it is, it does not appear to be subject to any restrictions or safeguards at all.

15. At the international level, APPG understands that the exchange of communications intelligence derived from foreign communications (i.e. communications of foreign countries) between the UK and the USA is governed by a multilateral agreement dating back to 1946 ('the UKUSA Agreement'). The full text of the UKUSA Agreement was disclosed in 2010 on the NSA website; it is possible that related documents, such as subsidiary arrangements, may remain secret.[10] The UKUSA Agreement contains only limited safeguards on the use of such intelligence, e.g. prohibiting its dissemination to entities that will exploit it for commercial purposes. The default position is that the exchange of intelligence will be "*unrestricted*" *[…] except when specifically excluded*". Art 3(b) provides:

    It is the intention of each party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon.

16. The APPG acknowledges the undoubted importance of intelligence-sharing but expresses concern at the virtually unfettered discretion that appears to be given to the Secretary of State and the security and intelligence agencies in this respect.

17. The disclosure to a foreign power of data relating to an individual is a significant interference with the Article 8 rights of that individual. Interferences with Article 8 are only permissible where they are necessary for one of several specified purposes (e.g. national security) and proportionate to that aim. An interference will not be proportionate if it is not 'in accordance with the law'; it is well-established that proportionality requires, at an absolute minimum, clear and foreseeable limits on the exercise of any executive power to interfere with rights (see e.g. *Malone v UK*[11]).

18. In the *Liberty* IPT case, the Tribunal held:

[10] I. Brown and D. Korff, '*Foreign Surveillance: Law and Practice in a Global Digital Environment*', [2014] EHRLR 243, fn 39.

[11] European Court of Human Rights, application no. 8691/79.

41 … We are satisfied that in the field of intelligence sharing it is not to be expected that rules need to be contained in statute … or even in a code … It is in our judgment sufficient that:

(i) Appropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an adequate indication of it (as per Malone*…)*

(ii) They are subject to proper oversight.

19. The IPT's judgment (and, similarly, the ISC Report) focuses primarily on the receipt of shared intelligence from the US by UK agencies. Neither looks in any depth at the current arrangements for sending intelligence data overseas. However, it is clear that - even by the IPT's modified standard set out above – the arrangements for the disclosure of data to foreign powers by UK agencies are not adequate for the following reasons.

20. First, the Secretary of State has a wide statutory discretion under RIPA to determine what safeguards, if any, must be applied to intercepted communications disclosed to foreign powers. Neither the Code nor any other public document constrains the exercise of this discretion.

21. Second, despite a written request from members of the APPG to the Foreign Secretary, the internal guidance on the passing of communications data by UK intelligence and security agencies to foreign powers has not been disclosed.[12] The failure to disclose relevant internal guidance was a significant factor in the IPT's finding of a violation of Art 8 and/or Art 10 in the *Liberty* case.[13]

22. Third, the UKUSA Agreement provides no meaningful safeguards on the sharing of intelligence data. The UKUSA Agreement was clearly drafted at a time when official state communications were more readily

[12] Available at: http://appgdrones.org.uk/wp-content/uploads/2014/08/Rt-Hon-Philip-Hammond-MP9-FINAL-3.pdf.

[13] Both the IPT Judgments and the ISC Report make reference to the existence of internal guidance on the *receipt* of intercepted data by UK agencies, but do not deal with guidance on the *disclosure* of intercepted data in any detail.

intercepted than the private communications of individuals. That distinction is no longer relevant. The default position under the Agreement is that intelligence will be shared save in exceptional circumstances; that is not compatible with the modern concept of proportionality. Finally, and in any event, it is not clear whether the Agreement applies to internal communications (as defined in RIPA) or the communications of private individuals at all; yet section 15(6) of RIPA clearly envisages that such communications might be shared with foreign powers.

23. For those reasons, it is very likely that the current framework relating to the sharing of communications intelligence fails the proportionality test.

24. The position is even more worrying in relation to metadata acquired under a section 22 authorisation, as there seem to be no limits at all on the sharing of such information (bar the broad requirements in sections 2 and 4 of the Intelligence Services Act 1994 and section 2 of the Security Service Act that any disclosure be necessary for the discharge of the agencies' functions).

25. Insofar as a policy choice has been made to exempt metadata from the (very limited) safeguards of section 15 of RIPA, the APPG disagrees with this approach. The APPG does not accept that disclosure of metadata is somehow more benign than disclosure of the contents of communications. Recent technological advances have largely elided the significance of the distinction between contents data and metadata. A great deal of highly sensitive information can be gleaned from metadata: as Liberty has put it, metadata paints "*a rich picture of what a person does, thinks, with whom, when and where*".[14]

26. US National Security Agency ('NSA') General Counsel Stewart Baker has said:

> *Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.*[15]

[14] *Liberty's Submission to the Reviewer of Terrorism's Investigatory Powers Review*, November 2014.
[15] See http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata.

27. General Michael Hayden, former director of the NSA and the CIA, has publicly stated:

    We kill people based on metadata.[16]

28. Restrictions on the disclosure of metadata should therefore be no less stringent than restrictions on the disclosure of the contents of communications.

29. In summary, the framework governing the disclosure of intercepted data to foreign powers needs to be considered and updated. In the meantime, relevant internal (or 'below-the-waterline', to use the language of the IPT) guidance should be disclosed, as APPG Officers have sought. It is noted that, in the Consultation Document, the Home Office accepts in principle that there ought to be "*a robust statutory framework for the use of such intrusive investigative powers*" and "*a strong system of safeguards in place*". An analysis of the ISC report is beyond the scope of this Submission; however the APPG notes the conclusion of the report: there is a pressing need for new legislation.[17]

30. The Home Office is invited to give particular consideration to the ISC recommendation that the circumstances in which data may be shared, including constraints on intelligence sharing, should be set out clearly and comprehensively by statute[18].

31. As further noted in the ISC Report, there is also an issue as to the adequacy of safeguards on the sharing and disclosure of intelligence reports prepared by the UK agencies (as distinct from raw intercept data). The default position appears to be that all such information is sharable.[19] Again, this falls outside the scope of the current consultation, which is concerned with the interception of communications, although

[16] Ibid.
[17] ISC Report, Annex A, para YY(g).
[18] At Zg
[19] ISC Report, para 243.

it is also a matter of concern to the APPG. To the extent that intelligence reports refer to identifiable individuals, they clearly interfere with the Article 8 rights of those individuals. For all the reasons outlined above, such interferences should be subject to strict safeguards. A default presumption that intelligence reports are 'sharable' would seem to be fundamentally incompatible with the UK's obligations under the ECHR.

32. It would be wise to consider different types of intercept and other data that may need different consideration in the statutory scheme; and the appointment of a person or team with responsibility to assess the risk that end-use of data may be unlawful.

'EXTERNAL' AND 'INTERNAL' COMMUNICATIONS

33. While the APPG's primary concern is with the sharing of intelligence data with foreign powers that carry out drone strikes, it also has an interest in the intermediary steps in the intelligence-gathering process leading up to the sharing of data.

34. The APPG therefore points out that there is a lack of clarity in the distinction drawn by RIPA between 'internal' and 'external' communications. The Code (as in previous drafts) emphasises that communications are <u>not</u> 'internal' by virtue of the fact that they pass through the British Island *en route* to their destination (para 6.5). It gives the specific example of an email sent from a person in London to a person in Birmingham, routed via foreign IP addresses, which is an 'internal' communication.

35. This is clearly correct, and consistent with the legal advice that the APPG has already seen. However, in the *Liberty* IPT case, Mr. Charles Farr, Director General of the Office for Security and Counter Terrorism in the Home Office, gave evidence that web searches on Google, 'tweets' on Twitter and public messages on Facebook were considered to be external communications. Mr. Farr's view was that the recipients of e.g.

a ‘tweet’ were not its readers but rather the Twitter web server. The APPG suggests that this is an overly technical interpretation of RIPA, not consistent with the approach to emails set out in the Code and not in the spirit of the legislation. The Code does not deal with this point.

36. In light of the increasing use of social media platforms as an alternative to conventional email, it would seem that treating social media messages as external communications could undermine the RIPA scheme, which gives greater protection to communications passing between people in the British Islands.

37. At the very least, the APPG suggests that the final draft of the Code set out expressly the Home Office’s position on web searches, tweets, Facebook messages, etc. Once that is clear, there will be scope for further informed debate.

FURTHER ACTION

38. Given the use to which intercepted data may be put once shared with foreign powers – *i.e.* the facilitation of drone strikes – the APPG requests that the Home Office critically evaluate the existing (i) statutory framework, (ii) practice, (iii) non-statutory safeguards and (iv) oversight provisions relating to the intelligence-sharing of intercepted data, either in parallel with or immediately following this consultation exercise. This would naturally require input from other Government departments, but as the department responsible for the regulation of data intercepted in the UK, it is the place of the Home Office to initiate such a review. For all the reasons set out above, the APPG considers that review and oversight of UK-US data sharing arrangements have been neglected.

39. The APPG considers that, as a minimum, the following is necessary:

    a. In granting a warrant, consideration must be given by the Secretary of State to the ultimate use to which intercepted information is to be put. The risk that data is or may be used to facilitate lethal drone strikes must be relevant to the assessment

of proportionality and considered not simply at the point at which data is to be shared with foreign powers, but at the time of its proposed interception. The Secretary of State must also be empowered to place appropriate constraints or conditions on the end-use of intercepted data at the time of granting a warrant. The same goes for the grant of authorisation for the interception of metadata pursuant to section 22 of RIPA. This should be set out in the Code.

b. The sharing of intercepted (and other) intelligence with foreign powers must in each case be subject to a formal, comprehensive framework – for example a bilateral agreement, annex to the 1946 agreement or a memorandum of understanding – setting out the uses to which data may be put, and those to which it may not be put.

40. The APPG hopes that the Home Office will also support its request to the Foreign and Commonwealth Office, made jointly with Professor Sir David Omand and Professor Michael Clarke, for disclosure of the Guidance that applies to the transfer of data available for use to target suspected terrorists outside traditional battlefields by the United States. Pending full review, and the implementation of proper statutory safeguards, disclosure of such 'Drones Guidance' is of critical importance and very much in the public interest.

41. The APPG further notes that the Obama administration in the US has engaged actively in high-level debate regarding the interception of data concerning US citizens, and is likely to be receptive to proposals for reform. In 2014 Timothy Edgar, who served under President Obama as the first director of privacy and civil liberties for the White House National Security Staff, engaged in debate with David Davis MP (and others) at an event held at Westminster. As Mr. Edgar subsequently put it in an email (disclosed with his permission):

*The only publicly available version of the existing agreement [*the UKUSA Agreement*] was declassified in 2010 and is available on the NSA's website. It is very much out of date. It would be worth thinking about*

what a new agreement would look like and how it would incorporate protections for privacy and civil liberties. The drones issue is only one of the most dramatic issues that highlight the effect that intelligence information has.

42. Finally, it would be worthwhile for the Home Office to consider critically the benefits of intercept data. The Consultation Document states that the Code is based on the premise that intercept material is a "*vital tool in the fight against terrorism and serious crime*". It asserts that "*since 2010, the majority of the MI5's top priority counter-terrorism investigations have used intercept capabilities in some form*". However, no in-depth analysis of the use and benefit of intercept material obtained through bulk collection appears to have been carried out. By contrast, a White House review group in the US has found that such data is not essential and could have been obtained by conventional means.[20] Detailed research by Peter Bergen at the New America Foundation has concluded that bulk phone records have had no discernible impact on preventing acts of terrorism.[21] The APPG invites the Home Office to commission comparable rigorous, independent research into the factual assertions that underpin the Code. This should in any event be done before a new Bill is drafted.

CONCLUSION

43. The APPG is concerned by the lack of statutory or other safeguards on the disclosure of intelligence data to foreign powers. In light of the IPT's judgment in the *Liberty* case it is highly likely that current arrangements – which give the executive a very wide discretion – are not ECHR-compliant. The lack of clarity in the law as it stands is particularly problematic in light of the lethal consequences of sharing data with foreign powers that use the data to carry out drone strikes against non-

[20] '*Liberty and Security in a Changing World*', December 2013, available at: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[21] 'Do *NSA's Bulk Surveillance Programmes Stop Terrorists?*', January 2013, available at: http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf

combatants. The implications of this demand careful review by the Home Office (as well as Foreign Office).

44. The APPG also takes the view that some of the intermediary steps leading up to the sharing of intelligence require clarification. The Code should state expressly whether the Home Office characterises web searches and messages on social media platforms as external communications. Moreover, the Code, and the legislative framework around it, should not assume that metadata is somehow more benign or less significant than the content of communications.

45. The APPG encourages the Home Office to implement rules that (i) compel the Home Secretary to consider the end-use of intelligence data at the stage of granting a warrant and (ii) limit the circumstances in which certain types of data may be disclosed to a foreign partner absent understanding and agreement as to the ultimate use. At the least, the Code should address the need to take end-use by a foreign partner into account.

46. More generally, the APPG suggests that more work needs to be done to investigate the benefits of bulk interception, given the significant level of interference with individual rights that it necessarily entails.

47. This Submission is not an official publication and may not represent the views of individual APPG members.

This submission is made by the following named officers, on behalf of the All Party Parliamentary Group on drones:

Chair: Tom Watson MP (Lab);
Vice Chairs: Baroness Stern (CB); David Davis (Con);
Treasurer: John Hemming MP (LD);
Secretary: David Anderson MP (Lab).

For any further information, please contact the APPG's Researcher Anna Thomas on anna.thomas@parliament.uk