Comments to IPCO on proportionality factors relating to bulk powers

Graham Smith

13 June 2018[1]

These comments are submitted in response to the open invitation of the Investigatory Powers Commissioner of 24 May 2018. They are made in the writer's personal capacity and should not be taken as representing the view of any client for whom the writer has acted or of Bird & Bird LLP, the firm in which he is a partner.

These do not constitute a comprehensive or exhaustive response, but discuss some points of particular interest to the writer.

1. IPCO QUESTIONS

1.1 The questions that IPCO poses are:

- What factors the Judicial Commissioners should take into account when considering whether the conduct proposed in a bulk warrant is proportionate?

- Is there any particular approach that the Commissioners should adopt when evaluating those factors, some of which may be competing?

1.2 These questions are, unsurprisingly in the light of the role of the Judicial Commissioners in approving warrants, specific to the conduct proposed in a given bulk warrant.

1.3 The human rights compatibility of UK bulk powers is under challenge in the European Court of Human Rights (*BBW, BIJ and 10 NGOs v UK* (RIPA s.8(4)) and in the pending Liberty judicial review of the Investigatory Powers Act. The issues raised in those challenges may overlap with the question of what factors should be taken into account when considering a particular warrant under the IPAct.

1.4 Whilst IPCO's questions concern all bulk powers, these comments are directed to bulk interception warrants.

1.5 The difficulties of assessing proportionality at a general level are illustrated by hypothetical Case Study A10/6 in the Bulk Powers Review, designed to illustrate when a bulk rather than a thematic EI warrant might be appropriate. It can be applied to all bulk powers. Example 2 states that:

"the Secretary of State cannot know or fully assess all of the interferences with privacy that will occur (both in relation to the cell members and innocent individuals whose devices will be affected) from the start to the end of the operation. The Secretary of State knows:

- the objective and the scale of the operation and what will be done in order to collect the initial 'pot' of data;

- that the information to be retrieved from the 'pot' of data will likely include the data of terrorists, that will lead to the cell, but also some data belonging to innocent individuals (given the software package is not exclusively used by terrorists); and

[1] Incorporating further corrections and clarifications, 28 June 2018.

- that further analytic work will be required leading to more refined searches on the initial 'pot' in order finally to discover and obtain the communications of the terrorist cell.

But at the point of issuing the warrant, the Secretary of State is not in a position to assess the necessity and proportionality of subsequent searches of the 'pot'. To ensure that all of those searches are carried out in accordance with privacy considerations, additional examination safeguards need to be in place."

1.6 The main proportionality assessment required under the Act is whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct (S.138(1)(c) and S.140(1)(b)).

1.7 The conduct authorised by a bulk interception warrant includes the securing, by any conduct described in the warrant, of selection for examination and of disclosure (S.136(4)(c) and (d)). Thus conduct securing "subsequent searches of the 'pot'", the proportionality of which the Case Study admits cannot be assessed at the time of issuing the warrant, is among the matters the proportionality of which the Act requires to be considered.

1.8 The Case Study suggests that safeguards are sufficient to square this circle. The main safeguards in the Act relating to searches of material acquired under a bulk interception warrant are contained in S.152. For secondary data under a bulk interception warrant they amount to:

- Restriction to selection for the operational purposes set out in the warrant (S.152(1)(a))

- A requirement that the selection for examination be necessary and proportionate in all the circumstances (S.152(1)(b))

1.9 For content (but not secondary data) there is a requirement to obtain a targeted examination warrant for a person known to be in the British Islands.

1.10 The assessment of proportionality at the time of issuing the warrant appears to depend in part on an assumption that the selection for examination will itself be proportionate as required by S.152(1)(b). Since the proportionality of individual selection decisions cannot be assessed at the time of issue of the warrant, the best that can presumably be done is to review the relevant safeguards.

2. SCOPE OF ANALYSIS OF PROPORTIONALITY

Conduct authorised by warrant includes safeguards on selection for examination and disclosure

2.1 At any event, since the conduct authorised by the warrant in relation to selection for examination and disclosure is necessarily constrained by the safeguards, it would seem to follow that JC review of the authorised conduct for proportionality should include (for bulk interception) the arrangements for safeguards under Ss.150 to 154 of the Act. That would appear to include review of the arrangements for ensuring that any selection for examination carried out is in fact necessary and proportionate. (See further below as to scope of conduct authorised by the warrant, para 2.8 et seq.)

2.2 That could bear on a variety of different kinds of selection for examination (subject to any questions as to which automated techniques do and do not amount to selection

for examination). These may vary in features such as intrusiveness and likelihood of false positives, with potential impact on proportionality. Examples include:

- Bearer selection (Bulk Powers Review, para 2.15)
- Filtering (Bulk Powers Review, para 2.16)
- Triage (Bulk Powers Review, para 2.18)
- Application of selectors in near-real time (Bulk Powers Review, paras 2.17 and 2.19(a))
- Complex queries (Bulk Powers Review, paras 2.17 and 2.19(b))
- Ad hoc queries by an analyst self-certifying that a search is proportionate.
- Provision of datasets designed to enable specific kinds of query to be made on them (Query Focused Datasets, e.g. KARMA POLICE, referred to in the Snowden documents)
- Pattern analysis/anomaly detection (BPR, p.147 ("changes in behaviour"); Case Studies A8/2 ("look for patterns of behaviour..."), A11/2 ("analyse patterns of behaviour"); ISC March 2015 Report: " GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security." (BPR, para 3.26); BPR para 4.8: "Anomaly detection – a technology-based process by which patterns in bulk data are identified and analysed to assist in the detection of e.g. malware and cyber-attack signatures. This is essential for Cyber Defence."; BPR para 5.46: "Bulk interception remained of value, despite the increasing use of encryption, and was noted to be particularly important in enabling target discovery and in pattern analysis."; BPR para 5.48: "detection work that was based on the use of a technology or on patterns of behaviour or movement."; BPR para 8.19: "analysis of BPDs may lead to the identification of patterns which reveal hostile activity"; and see BPR para 9.15.)

2.3 See further Section 3 below 'Computer processing'.

Impact of general duty of privacy on scope

2.4 The Act (s. 140(1)) requires the Judicial Commissioners to review the SoS's conclusions in relation to a bulk interception warrant as to the following matters:

(a) Whether the warrant is necessary on the statutory grounds (national security etc)

(b) Whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct

(c)(i) Whether each of the specified operational purposes is a purpose for which examination of intercepted content or secondary data obtained under the warrant is or may be necessary.

(c)(ii) Whether the examination of intercepted content or secondary data for each such purpose is necessary on any of the [statutory] grounds for which the SoS considers the warrant to be necessary

(d) Any matter taken into account in relation to overseas operators under S.139.

2.5 The Judicial Commissioner must consider these matters with a sufficient degree of care as to ensure that the JC complies with the general duty of privacy under S.2. Thus the JC must have regard to:

(2)(a) Whether what is sought to be achieved by the warrant could reasonably be achieved by other less intrusive means

(2)(b) Whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant is higher because of the particular sensitivity of the information

(2)(c) The public interest in the integrity and security of telecommunication systems

(2)(d) Any other aspects of the public interest in the protection of privacy.

2.6 These duties apply so far as they are relevant in the particular context and are 'subject to the need to have regard to other considerations that are also relevant in that context' (S.2(3)(b)) Those other considerations may, in particular, include other considerations that are relevant to whether the conduct that would be authorised or required by the warrant is proportionate, the requirements of the Human Rights Act 1998 and other requirements of public law (S2(4)(c) to (e)).

2.7 Thus although the consideration of proportionality required by S.140(1)(b) itself is quite specific, the requirement to comply with the general privacy duty by virtue of S.2 appears as a matter of language to suffuse all the matters under S.140 with a requirement to consider proportionality. Whether that would have any practical consequences is unclear. The Code of Practice refers at 6.25 and 6.26 only to S.140(1)(b) and S. 2(2)(a).

Conduct authorised or required by the warrant

2.8 Ss. 138(1)(c) and 140(1)(b) refer to having regard to proportionality of conduct that would be "authorised by" the warrant. S.2(4)(c)(i) refers to conduct "authorised or required by" the warrant. IPCO's question refers to conduct "proposed in" a bulk warrant.

2.9 Conduct authorised by a warrant may include both conduct described in the warrant and conduct authorised by the warrant but not described in it.

<u>Conduct authorised by and described in the warrant</u>

2.10 The requirements for the contents of a bulk interception warrant are derived from S.136 and S.142. S.136 specifies the conditions that a warrant must meet in order to be a bulk interception warrant. It includes a requirement to describe in the warrant the authorised conduct by which certain activities will be secured.

2.11 The conduct description aspects are set out in the following table.

S.136(4)	S.142
authorises or requires the person to whom it is addressed to secure, *by any conduct described in the warrant*, any one or more of the following activities:	
(a) the interception, in the course of	

	their transmission by means of a telecommunication system, of *communications described in the warrant*;	
	(b) the obtaining of secondary data from communications transmitted by means of such a system and *described in the warrant*;	
	(c) the selection for examination, *in any manner described in the warrant*, of intercepted content or secondary data obtained under the warrant;	
	(d) the disclosure, *in any manner described in the warrant*, of anything obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.	
		(3) specify the operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination

Conduct authorised by but not described in the warrant

2.12 Some authorised or required conduct may be relevant to proportionality but not described (or at least not required by the Act to be described) in the warrant.

2.13 Thus under S.136(5) a bulk interception warrant authorises (in addition to the conduct described in the warrant):

(a) Any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including:

(i) The interception of communications not described in the warrant and

(ii) Conduct for obtaining secondary data from such communications

2.14 Since this conduct falls within both S.140(1)(b) and S.2(4)(c)(i), the Judicial Commissioner is required to consider its proportionality. *Ex hypothesi* (given the terms of S.136(5)) it is conduct that is not described in the warrant. However the Code of Practice (6.20(c)) states that the warrant *application* must describe the conduct (*including the interception of other communications not specifically identified by the warrant as set out at section 136(5)*) it is necessary to undertake in order to carry out what is authorised or required by the warrant.

2.15 Conduct authorised under S.136(5) can be as important, if not more so, than conduct described in the warrant. The existence of 'by-catch' material, both content and (as it was known under RIPA) related communications data, was a significant point of controversy in the *Liberty/Privacy* case challenging RIPA S.8(4) in the Investigatory Powers Tribunal.

2.16 The Judicial Commissioners are required by the Act to go outside the conduct described in the warrant and consider the proportionality of other conduct authorised by the warrant but not described in it.

2.17 The Code of Practice (6.20(c)) requires such other conduct to be described in the warrant application. Is that sufficient, or will Judicial Commissioners need to be able to ascertain and satisfy themselves as to the existence and nature of such other conduct?

Safeguards

2.18 The conduct authorised by the warrant includes selection for examination and disclosure (S.136(4)(c) and (d)). The SoS is required under S.138(1)(e) to consider that satisfactory arrangements made for the purposes of the examination and disclosure safeguards under S.150 and 152 are in force in relation to the warrant. The proportionality review should include review of those safeguards, since (a) they place limits on the conduct authorised under the warrant and (b) they themselves contain a proportionality requirement in relation to selection for examination (S.152(1)(b)).

3. COMPUTER PROCESSING

3.1 There may be uncertainty as to the status under the Act of the computer processing that takes place between the act of interception and making available to an analyst. There appear to be four options, any one of which may apply depending on the processing technique being deployed:

- The processing constitutes 'selection for examination' and is thus required to be described in the warrant under S.136(4)(c).
- The processing constitutes 'disclosure' and is thus required to be described in the warrant under S.136(4)(d).
- The processing constitutes conduct to secure one of the activities set out in S. 136(4) (interception, obtaining of secondary data, selection for examination or disclosure) and is thus required to be described in the warrant by virtue of the opening wording of S.136(4) ("...secure, by any conduct described in the warrant").
- The processing is 'other conduct' authorised by the warrant under S.136(5) and thus is not required to be described in the warrant (but under para 6.20(c) of the Code of Practice ought to be described in the application for the warrant).

3.2 If processing does not fall under one of these heads there appears to be no other basis on which it can be authorised.

3.3 Whatever the status under the Act of any particular processing technique, it will inevitably be relevant to the proportionality assessment. Intermediate processing techniques will affect the quantity and nature of the material passed through to storage and made available to human analysts or for computerised analysis (such as pattern analysis). Computerised analysis may of itself point the finger of suspicion, requiring further processing if the finger is to be withdrawn (or not) (see Bulk Powers Review Case Study A9/7).

3.4 Processing to extract items from the body of communications and treat them as secondary data under S.137(5) is likely to be relevant to proportionality. If the

extracted material would be likely to be regarded as content from an independent human rights standpoint (which may not draw the same line between content and metadata as that defined under this part of the Act) that may affect the proportionality assessment differently from if it were properly regarded as communications data (albeit there appears to be increasing appreciation in human right law of the extent to which communications data can reveal aspects of private life).

3.5 The way in which material is stored may be relevant to proportionality, at least if it is structured so as to enable particular kinds of queries, of identifiable degrees of intrusiveness, to be made (cf para 2.2, above, regarding Query Focused Datasets).

3.6 Seeded and unseeded analytical techniques may be viewed differently from a proportionality point of view. Seeded analysis starts with a known 'bad' device, person or selector. Unseeded pattern analysis relies on (a) an assessment of what constitutes 'normal' (b) thus requiring collection and analysis of bulk data of non-suspects in order to arrive at a 'normal' baseline (c) design of pattern matching/anomaly detection algorithms (d) confidence that such algorithms are unbiased and have low false positive rates. See examples of apparent use of such techniques in the Bulk Powers Review cited under Pattern analysis/Anomaly detection above.

3.7 The kinds of risks associated with the use of such techniques are set out in the judgment of the CJEU in the *Canadian PNR Agreement* case (paras 168 to 174) and the Opinion of AG Mengozzi referred to in the judgment.

3.8 Generally, target discovery (unseeded) as opposed to target development (seeded) seems likely to give rise to greater proportionality issues. However the terms do not appear to be used completely consistently in the Bulk Powers Review. For instance, detection of unknown members of a network may be described as target discovery or target development (as in A8/2), depending on whether the 'target' is regarded as (a) the unknown individuals or (b) the network.

4. USE OF OTHER THAN OVERSEAS-RELATED COMMUNICATIONS AND SECONDARY DATA

4.1 The main purpose of a bulk interception warrant must be the interception of overseas-related communications, the obtaining of secondary data from such communications or both (S.136(3)). However it is inevitable that in the process of collecting external communications in bulk, internal communications will also be scooped up. That, and obtaining secondary data from such communications, is authorised by S.136(5). Like RIPA before it, the Act does not require the intercepting agency to discard or filter out such incidentally acquired communications.

4.2 As the IPT said in *Liberty/Privacy International* at [95]:

> "the relevance of the internal/external distinction has no relation to the s.16 examination, when a communication may be accessed and read..." and at [101(i)] "All communications, whether they be external or internal, intercepted by s.8(4) warrant come to be considered for examination by reference to s.16 of RIPA .... It is that section which does ... the "heavy lifting"."

4.3 Consistently with this scheme, the examination safeguards in S.152 of the IPAct make no reference to the overseas-related main purpose of the bulk interception. The purpose limitation is not carried through to examination.

4.4 The greatest impact of the main interception purpose not being carried through to examination is on secondary data, for which there is no requirement to obtain a targeted examination warrant.

4.5 Whilst the Act does not carry through the overseas-related purpose limitation from acquisition to use of the material, is the limited nature of the initial main purpose nevertheless relevant to proportionality?

4.6 In this regard it is pertinent to recall the government's justification in *Liberty/Privacy International* for the lack of restrictions on the use of related communications data (as it was termed under RIPA). It was that the data could be used to ascertain whether a person was inside or outside the British Islands. The IPT held:

> "We conclude that although the *Weber* requirements do extend to protection in respect of communications data, for the reasons set out by the Respondents there is such protection or safeguard by reference to s.15, and, insofar as there is, in the particular circumstances governed by s.16, greater protection in certain respects for communications than for communications data, that difference is justified and proportionate2 by virtue of the use of that communications data for the purpose of identifying the individuals whose intercepted material is to be protected by reference to s.16(2)(a)."

4.7 The same justification was put forward by the Minister in the IPAct Commons Committee debate:

> "Authorisation for persons in the UK does not apply to secondary data, because it is often not possible to determine the location of a person without taking those data. The reason why it looks like there is an inconsistency in respect of a set of data—or it might be perceived that way, without fuller consideration—is that, in relation to secondary data, it is not always possible to determine where someone is until the secondary data have been collected."

4.8 The uses of bulk secondary data illustrated in the Bulk Powers Review make no claim to be limited to ascertaining whether an individual is inside or outside the British Islands. The uses go far wider than that.

4.9 It also seems that (by contrast with content) little or no filtering may be carried out on acquired secondary data. The ISC Report of March 2015, para 134(3), said:

> “Related CD (RCD) from interception: GCHQ’s principal source of CD is as a by-product of their interception activities, i.e. when GCHQ intercept a bearer, they extract all CD from that bearer. This is known as ‘Related CD’. GCHQ extract all the RCD from all the bearers they access through their bulk interception capabilities...”).

4.10 These all appear to be factors potentially relevant to the proportionality assessment in relation to bulk secondary data.

---

2 The question before the Tribunal was whether RIPA S8(4) was 'in accordance with the law'. However the Tribunal also mentioned proportionality.