SUBMISSION OF Philip Glover, PhD Candidate, School of Law, University of Aberdeen. The views submitted are mine alone. My research is funded by the Arts & Humanities Research Council.

EXECUTIVE SUMMARY

My submission attempts to address each of the questions within questions posed in the ISC consultation. However its principal focus is on what I perceive to be flaws in the current legislative framework; ISA 1994 and RIPA 2000. It is felt that these statutes do not adequately envisage authorize or regulate; (1) the blanket 'mining' of UK residents' communications or (2) the acquisition by UK intelligence-gathering bodies of extra-jurisdictionally obtained intercepted material.[1] This leaves these important areas open to criticism as being conducted in a manner that is not 'in accordance with the law.' These leaves the UK in the embarrassing position of facing ECtHR censure when we are a purported bastion of the rule of law. It is submitted that any flaws in the framework are mainly attributable to poor drafting, and that replacement legislation should not only adopt a fixed definition of national security, but also separately regulate covert privacy intrusions on this particular ground.

(1) The collective right to security must always assume primacy over the individual right to privacy. No one can credibly argue that a State (through its intelligence-gathering bodies) should not award itself a "clear basis in law"[2] under which it can interfere with certain individual privacy rights on strictly delineated grounds.
(2) My view is that Art.8 privacy intrusion by States takes two principal forms with which most UK residents can identify.
    (a) **Overt privacy intrusion**- e.g. Surveillance cameras, security measures at airports etc. Whilst these impinge upon what the average UK resident would feel are their reasonable expectations of privacy, they are generally passively accepted in UK society as representing overt measures of generic (rather than targeted) national security protection and crime prevention.
    (b) **Covert privacy intrusion**- wherein the State (through its intelligence or evidence-gathering bodies) intrudes on any aspect of a UK resident's (or group of UK residents') private life, family life or correspondence, ***without their knowledge***.
(3) Internet communications are no different from any other form of human communication. They represent the most recent development in the means by which humans freely express themselves in line with their ECHR Art.10 rights, in the reasonable expectations of an ECHR Art.8 right. Interception powers should therefore extend to Internet communications. *Any* covert

[1] i.e. the content of UK residents' communications that have been intercepted outside the UK jurisdiction by non-UK intelligence-gathering bodies.
[2] As redefined in *Iordachi v Moldova* (2012) 54 E.H.R.R.5

intrusion wherein what UK residents reasonably expect to be their private communications (made by *any* technological means) are intercepted, listened to, monitored and/or recorded, should be envisaged, authorized and regulated in UK legislation *in the same way*. It follows that when drafting interception of communications legislation, those involved should concentrate less on the technical means or *type* of communication to be interfered with (e.g. post, telecommunications, internet, satellite etc.) but rather concentrate on the fact that a covert privacy intrusion involving interception of a person or group's communications *is* to be authorized, having regard to the contemporary ECtHR jurisprudence as to necessity and proportionality. This would remove the increasingly absurd distinction between obtaining the contents of communications via interception and obtaining them through a 'bug' or other technical device. It would also prevent domestic courts having to contend with "what constitutes an interception" etc. It would additionally future-proof the legislation against technological developments.

(4) No one can cogently argue against the need (particularly since 9/11) for States (including the UK) to monitor communications (internal and external) to protect national security. However a significant obstacle to regaining the electorate's trust is that the UK legislature repeatedly declines to define "national security." Whilst so doing might be difficult, in failing to do so, no clear parameters are placed on the purposes for which covert privacy intrusion in the UK can potentially be undertaken. This has a huge impact on trust. 'National security' should encompass the protection of infrastructure required for the UK to function normally as a democracy, its economic stability and the prevention of terrorism. The term should not be left undefined and left open to varying interpretations of Governments that come and go with each election, or by intelligence-gathering body chiefs insufficiently restrained by law and/or oversight. As long as the UK fails to clearly delimit in domestic law the grounds on which interception can be undertaken, room remains for valid criticism and suspicion that the State engages in clandestine interception beyond RIPA's stated purposes. As national security remains the sole preserve of Member States, there should be no difficulty outlining to the ECtHR that such measures have a clear basis in domestic law and that the means by which they are undertaken are necessary in a democratic UK and are proportionate to the direct threat posed to the effective functioning of the democratic infrastructure of the UK by e.g. Al-Qaeda, cybercrime, economic crime and other terrorism threats.

(5) The distinction between data and communications is becoming increasingly blurred. Communications data can actually build a far more accurate and detailed intelligence picture of a person than might be achieved through interception. Therefore covert Art.8 privacy intrusion by intelligence/evidence-gathering bodies for the purposes of acquiring data should not necessarily be authorized under a different process than

interception, particularly where such data acquisition is being covertly sought on 'protection of national security' grounds.

(6) Where communications data is sought as part of evidence-gathering for a criminal prosecution, power to obtain it should be located within the wider powers to secure and preserve evidence currently contained in PACE. This is because the communications data represents no more than another form of evidence, and will be overtly 'searched for' and retrieved by the relevant investigating body. Where however, communications data is being sought to build an intelligence picture unbeknown to the communicator (i.e. covertly), power to do so should remain framed in dedicated State covert-privacy intrusion legislation. Just as the State is covertly intruding on the Art.8 privacy right of a UK resident when it intercepts communications of any *type*, the same right is being covertly infringed on the same grounds for the same purpose by the State when it seeks to build an intelligence picture through the covert acquisition of communications data. A citizen will feel no less violated if he discovers the State has been acquiring his communications data and building a picture of his life, than if he discovers the State has been monitoring his communications.

b) It is my view that the legal framework which governs the security and intelligence agencies' access to the content of private communications is unfit for purpose. This is because two legal questions have arisen out of the Snowden disclosures. Both are the subject of legal proceedings recently initiated in the ECtHR.[3] The first relates to the quality of law[4] and proportionality (as measured against existing ECtHR jurisprudence regarding secret State surveillance)[5] of what is described as "generic GCHQ Intercept."[6] This question replicates that asked of the ECtHR in *Liberty and others v United Kingdom,*[7] albeit in relation to mass interception of external communications carried out under certificated warrants issued under RIPA 2000's predecessor, the IOCA 1985. The ECtHR found that the IOCA 1985 provisions lacked sufficient clarity to protect against abuse of power and that there had been a violation of Article 8 ECHR.[8] They additionally criticised the UK executive's virtually unfettered legal discretion in the area of external

[3] *Big Brother Watch, Open Rights Group, English PEN and Dr Constance Kurz v UK,* Application No. 58170/13

[4] *Big Brother Watch, Open Rights Group, English PEN and Dr Constance Kurz v UK,* Application No. 58170/13, 49-61

[5] Including, but not limited to, *Malone v UK* (1985) 7 E.H.R.R. 14, *Huvig v France* (1990) 12 E.H.R.R. 528, *Weber v Germany* (2008) 46 E.H.R.R. SE5, *Liberty and others v UK* (2009) 48 E.H.R.R. 1 and *Iordachi v Moldova* (2012) 54 E.H.R.R.5

[6] *Big Brother Watch, Open Rights Group, English PEN and Dr Constance Kurz v UK,* Application No. 58170/13, at 13.

[7] *Liberty and others v United Kingdom,* Application No.58243/00 (2009) 48 E.H.R.R. 1

[8] *Liberty and others v United Kingdom,* Application No.58243/00 (2009) 48 E.H.R.R. 1, [69-70]

communications interception,[9] ultimately holding that the UK's position was not "in accordance with the law."[10] Given that RIPA 2000's certificated warrant provisions essentially replicate those criticised in *Liberty*, and indeed preserve the validity of IOCA 1985 certificated warrants,[11] it appears, despite the adverse ruling, and the recommendations that followed it,[12] that nothing has really changed.

A more pressing problem lies, I feel, in the acquisition of extra-jurisdictionally obtained intercepted material, as neither the ISA 1994 or RIPA 2000 appear to envisage, authorise or regulate it.

The ISA 1994, section 3 and the acquisition of extra-jurisdictionally obtained intercepted material

This can be read as providing the legal basis for GCHQ to, *inter alia*, intercept all currently known forms of electronic communication, transmitted from or to any location in the world. This is evidenced by the absence of an express territorial limitation to their activities that is present in RIPA 2000.[13] It gives effect to the worldwide listening brief that GCHQ have possessed since the early 20th century and which forms the basis of their post-WWII remit as acknowledged in the UKUSA intelligence-sharing agreement.[14] Knowledge of GCHQ's worldwide monitoring brief, and of the existence of a legal basis for undertaking it, is in the public domain and is not disputed herein.[15] It is, in my view, entirely justifiable on grounds of protecting the national security of the UK. The problem (already highlighted) is that the UK continues to refuse to constrain 'national security' within a clear definition, thereby legitimising and fuelling civil libertarian criticisms and conspiracy theories.

GCHQ's mandate under the ISA 1994, section 3 is:

> To monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions [i.e. communications and communications-handling equipment] and to *obtain* and *provide* information derived from or related to *such emissions* or equipment and from encrypted material...[16]

---

[9] *Liberty and others v United Kingdom*, Application No.58243/00 (2009) 48 E.H.R.R. 1, [64]
[10] *Liberty and others v United Kingdom*, Application No.58243/00 (2009) 48 E.H.R.R. 1, [69]
[11] RIPA 2000, s.82(4) to (6) "Amendments, repeals and savings."
[12] See for example B. Goold, 'Liberty and others v The United Kingdom: a new chance for another missed opportunity' (2009) (Jan) P.L. 5
[13] See RIPA 2000, s.2(4) "definition of interception" which limits the communications to be intercepted to those within the UK
[14] UKUSA Agreement <http://www.nationalarchives.gov.uk/ukusa/> accessed 17th December 2013
[15] See, in general, Richard. J. Aldrich, GCHQ (Harper Press, 2011)
[16] ISA 1994, s.3(1)(a) Italics are the author's emphasis

My view is that the phrase "to obtain and provide information derived from or related **to *such emissions or equipment*** and from encrypted material" expressly limits the obtaining and provision of information derived from or related to emissions, equipment or encrypted material that have been monitored or interfered with *by GCHQ themselves*. It is submitted that this drafting cannot be construed any other way. It expressly and unreservedly permits the *provision* of information derived from or related to GCHQ's lawful activities (thereby giving sufficiently legal effect to the UK's UKUSA Agreement obligations) and places no limitations or safeguards as regards prospective recipients.[17] However, it simultaneously reserves and limits the *obtaining* (or acquisition) of 'information' to that which has been derived from or related *to those same GCHQ activities*. "Such" is therefore the crucial word that thereby prevents the acquisition of extra-jurisdictionally obtained intercepted material being given sufficiently clear statutory authority under section 3. On this interpretation, read either in isolation, or in conjunction with the conduct authorised in certificated warrants under RIPA 2000, section 8(4)-8(6), the ISA 1994, section 3 does not envisage, authorise or regulate the *acquisition* by GCHQ of extra-jurisdictionally obtained intercepted material from any extra-jurisdictional intelligence-gathering source.

RIPA 2000 and the acquisition of extra-jurisdictionally obtained intercepted material

RIPA 2000 is territorially limited to interceptions[18] undertaken *in the UK,*[19] by *UK* intelligence-gathering bodies.[20] It follows that an interception undertaken outside the UK's jurisdiction (e.g. by the NSA) will not constitute an interception within the meaning of the Act. An interception warrant cannot authorise an interception outside the UK's jurisdiction, and cannot be issued to any intelligence-gathering body outside the closed list in section 6(2). RIPA 2000 simply does not envisage, authorise or regulate interception of UK residents' communications by extra-jurisdictional intelligence-gathering bodies such as the NSA. This is supported by the relevant Explanatory Note,[21] and in a recent statement of the Interception Commissioner,[22]

[17] This gives implicit recognition to the fact that intelligence reports are shared by GCHQ under the UKUSA agreement
[18] RIPA 2000, s.2(2)
[19] RIPA 2000, s.2(4)
[20] RIPA 2000, s.6(2)
[21] RIPA 2000, Explanatory Notes, at [30]
[22] Sir Anthony May

who stated "Part I Chapter I of RIPA provides the statutory authority for lawful interception that takes place *in the British Islands*."[23] This does not necessarily conflict with GCHQ's worldwide interception mandate in the ISA 1994, section 3. Rather, it regulates any interceptions of UK residents' internal or external communications that GCHQ undertake *in the UK* by requiring them to seek an interception warrant.

What conduct is authorised by an interception warrant

RIPA 2000, section 5(1) initially provides that an interception warrant (of either type) may authorise or require its recipient, *by any such conduct as may be described within it*, to secure, *inter alia*, the interception of [such] communications in the course of their transmission [either postal or telecommunications based] as may be described in the warrant,[24] and/or to secure the *disclosure*, in such manner as may be described, of intercepted material obtained by the interception authorised or required by the warrant, and of related communications data.[25] The Explanatory Note accompanying section 5(1)(d) adds nothing of substance to the subsection, meaning that no limitation appears to be placed on who the issuing Cabinet Secretary may authorise or require the interception warrant recipient to secure the disclosure of intercepted communications or related material to.[26] The scope of 'conduct' is expanded upon in section 5(6) and encompasses significantly more than the technical acts of interception and listening/recording. It includes; all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake to do what is expressly authorised or required by the warrant,[27] conduct for obtaining related communications data[28] and conduct by any person who is providing

[23] Interception of Communications Commissioner Office, Sir Anthony May's response to the Article published in the Independent.< http://www.iocco-uk.info/sections.asp?sectionID=8&chapter=4&type=top> [accessed July 19, 2013].
[24] RIPA 2000, s5(1)(a)
[25] RIPA 2000, s5(1)(d). s.5(1)(b) and (c) are omitted from consideration for present purposes as they relate to interception of communications undertaken in relation to international mutual legal assistance agreements. Although the UK and US are parties to such an agreement, its scope makes no express reference to such assistance extending to the interception of communications. More importantly however, RIPA 2000's Explanatory Notes state that section 5 (1) (b) only refers to international mutual assistance agreements *designated under Section 1(4).* The only agreement so designated is the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.
[26] RIPA 2000, Explanatory Note [54] states that this subsection "allows for the disclosure of intercepted material and related communications data in a manner described by the warrant."
[27] RIPA 2000, s.5(6)(a)
[28] RIPA 2000, s.5(6)(b)

assistance in facilitating the interception [29] (usually communications service providers).[30]. It can be seen that the conduct (i.e. the technical/physical means) by which the applicant intelligence-gathering body proposes to obtain the intercepted material is not circumscribed. This usefully 'future-proofs' this particular provision against technological developments. All that section 5 requires is that a description of the proposed conduct is included in the body of the interception warrant.

However, despite the apparently unfettered scope of conduct authorised for achieving the stated purpose(s)[31] of either both warrant variants, limitations can be discovered. Firstly, the recipient UK intelligence-gathering body, using whatever conduct it deems appropriate and which will be described in the warrant, is authorised to secure only the interception of *such communications as may be described in the warrant*.[32] It has already been shown that for both interception warrant variants, these can only be communications for which the interception will be undertaken *in the UK*, i.e. UK residents' communications that have been *sent or received in the UK.* [33] An interception warrant can therefore never cover extra-jurisdictional interceptions. It follows therefore that nothing in any of the section 5 provisions regarding conduct can be construed as authorising, requiring or securing the acquisition of extra-jurisdictionally obtained intercepted or of related communications data. It appears that (as in the ISA 1994, section 3) the drafting of RIPA 2000, section 5 envisages that intercepted material might require to be *disseminated* to interested parties whether in the UK or not (again giving statutory recognition to the UK's perceived obligations under the UKUSA agreement) [34] but equivalent provision for circumstances wherein intercepted material obtained outside the UK might be *acquired* is not so envisaged.

RIPA 2000's definitions of what constitutes an interception (section 2(2) and 2(4)), its express provisions as to what conduct is permissible under interception warrants (section 5), its limitations as to who may apply for an interception warrant (section 6(2)), its definition of "intercepted material" (section 20), the stated purposes of both types of interception warrant (section 8, read alongside section 5(3)) and the associated intercepted material safeguards at sections 15 and 16 all combine to

[29] RIPA 2000, s.5(6)(c)
[30] RIPA 2000, s11
[31] RIPA 2000, s.5(3)
[32] RIPA 2000, s5(1)(a)
[33] RIPA 2000, s.2(2) and s.2(4). See also s.20 as regards external communications. The Act's drafting envisages that these too will be intercepted in the UK
[34] RIPA 2000, s.5(1)(d)

envisage, authorise and regulate only the interception of UK residents' communications undertaken *in the UK*, by UK-based intelligence-gathering bodies. These limitations (again a direct consequence of drafting) mean that the acquisition of extra-jurisdictionally obtained intercepted material by UK intelligence-gathering bodies has no legal basis within RIPA 2000. The safeguard provisions of the Act that relate solely to intercepted material originating in the UK as contained in sections 15 and 16 are instead being applied to extra-jurisdictionally obtained intercepted material upon its receipt, in line with administrative guidance and Ministerial oversight.

It is submitted therefore, that the acquisition of extra-jurisdictionally obtained intercepted material by UK intelligence-gathering bodies is not being undertaken in accordance with the law, when contemporary ECtHR jurisprudence regarding secret State surveillance is taken into consideration.

ECtHR principles relating to member states' interception of communications "in accordance with the law.

For the acquisition of extra-jurisdictionally obtained intercepted material to be "in accordance with the law," the most recent ECtHR observations in *Iordachi v Moldova*[35] restate that the ECHR, Article 8(2) interference with the right to a private life that interception of communications has been repeatedly held to constitute should firstly "have some basis in domestic law."[36] Furthermore, *Iordachi* reiterates the ECtHR's position on "the quality of the law in question, [for present purposes the ISA 1994 and RIPA 2000] requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him."[37] It can confidently be said that, given the absence of clear express statutory provision for the acquisition of extra-jurisdictionally obtained intercepted material, compounded by the total absence of public access to guidance as to how, when, why and for what purposes it might be acquired by UK intelligence-gathering bodies, that the current UK position appears wide open to ECtHR censure as regards compatibility with the rule of law and accessibility.

[35] *Iordachi v Moldova* (2012) 54 E.H.R.R. 5
[36] *Iordachi v Moldova* (2012) 54 E.H.R.R. 5 [37]
[37] *Iordachi v Moldova* [2012] 54 E.H.R.R. 5 [37]