BINGHAM CENTRE FOR THE RULE OF LAW

THE INVESTIGATORY POWERS REVIEW BY THE INDEPENDENT REVIEWER OF TERRORISM LEGISLATION

Submission by the Bingham Centre for the Rule of Law

November 2014

www.binghamcentre.biicl.org

Bingham Centre for the Rule of Law
Submission to the Investigatory Powers Review
November 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Bingham Centre for the Rule of Law welcomes the review of investigatory powers by the Independent Reviewer of Terrorism Legislation under Section 7 of the Data Retention and Investigatory Powers Act 2014 (DRIPA). The Centre's written evidence has been authored by Dr Eric Metcalfe, a Fellow of the Bingham Centre. The response draws on contributions made by experts on investigatory powers during a seminar organised by the Centre on 1 October 2014.

The Bingham Centre acknowledges that the government has a particular responsibility to protect the public from serious crime, including acts of terrorism. It therefore also accepts that in narrowly-defined and exceptional circumstances the police and intelligence services will require the power to intercept private communications, access communications data and other intrusive surveillance. In such circumstances, the need for secrecy will necessarily involve some curtailment of both the right to a fair hearing and the right to an effective remedy of those affected by the surveillance. Nonetheless, the government does not enjoy an unlimited discretion to undertake surveillance. On the contrary, the highly exceptional nature of investigatory powers means that it is all the more important to ensure that the prevailing legal framework in respect of such powers complies with the rule of law. In particular, the law must be accessible and sufficiently certain, provide adequate protection for fundamental rights and comply with the United Kingdom's obligations under international law.

At present, the Bingham Centre has concerns about the extent to which the statutory framework governing investigatory powers falls short of these benchmarks. Accordingly, this response makes a number of recommendations that are all directed towards enhancing adherence to the rule of law and our common law constitution. It makes recommendations about the framework under the Regulation of Investigatory Powers Act 2000 (RIPA), specifically with respect to the interception of communications, the use of intercept evidence, communications data, intrusive surveillance, encryption keys, and oversight. It also makes recommendations with respect to data retention under DRIPA.

Our recommendations are:

(i) A single, comprehensive statutory framework should govern the use of intrusive surveillance powers by public bodies. In particular, no public body should have the power to access communications data save by way of this framework.

(ii) Judicial authorisation should be required before any public body intercepts communications, accesses communications data, uses intrusive surveillance (including a covert human intelligence source), issues an encryption notice or a retention notice. The authorising judge should also have the power to direct the appointment of a special advocate to represent the interests of the subjects of surveillance in appropriate cases.

(iii) The existing power to intercept external communications under section 8(4) RIPA should be repealed. At the very least it should be severely curtailed. All warrants and

authorisations must be founded on the reasonable suspicion of the authorities that a particular individual has been involved in serious criminal activity.

(iv) The statutory definition of 'intrusive' surveillance should be tightened to include *any* covert surveillance that either involves or is likely to involve a significant interference with a person's privacy.

(v) The ban on the use of intercept material as evidence in criminal and civil proceedings should be lifted.

(vi) The number of public bodies able to access communications data should be curtailed.

(vii) The oversight functions currently discharged by the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner should be combined into a single statutory oversight body. This body's remit should include oversight of the use of all surveillance powers by public bodies.

(viii) Any person who has been the subject of covert surveillance by a public body should be notified of that fact within a reasonable period following the conclusion of the surveillance, unless a judge is satisfied that that individual's right to an effective remedy is outweighed some specific investigative need that would otherwise be prejudiced by the disclosure.

(ix) The Investigatory Powers Tribunal should be granted the power to appoint special advocates to represent the interests of excluded parties, as well as make a declaration of incompatibility under section 4 of the Human Rights Act. Its procedural rules should also be relaxed to allow much greater disclosure to complainants who have been the subject of surveillance, in order that they may bring an effective challenge. This should include sufficient disclosure to enable them to give effective instructions to the special advocate representing them in any proceedings from which they have been excluded. The unsuccessful party should also have the right of appeal to the Court of Appeal on a point of law.

(x) The statutory requirement that candidates for the Intelligence and Security Committee must first be nominated by the Prime Minister in order to be eligible for election should be repealed, as should the power of the Prime Minister to prevent the Committee from publishing material that it considers to be in the public interest to disclose.

INTRODUCTION

1. The Bingham Centre for the Rule of Law welcomes the review of investigatory powers by the Independent Reviewer of Terrorism Legislation under section 7 of the Data Retention and Investigatory Powers Act 2014 (DRIPA). The Centre's response is authored by Dr Eric Metcalfe (Fellow of the Bingham Centre) but also draws upon contributions from experts in a seminar organised by the Centre on 1 October 2014 and has input from senior Bingham Centre staff. The 1 October seminar programme and list of attendees is attached as an appendix.

About the Bingham Centre

2. The Bingham Centre for the Rule of Law was launched in December 2010 and is devoted to the study and promotion of the rule of law worldwide. Its focus is on understanding and promoting the rule of law; considering the challenges it faces; providing an intellectual framework within which it can operate; and fashioning the practical tools to support it. The Centre is named after Lord Bingham of Cornhill KG, the pre-eminent judge of his generation and a passionate advocate of the rule of law. It is part of the British Institute for International and Comparative Law, a registered charity based in London.

3. The Bingham Centre has a particular interest and expertise in the law governing investigatory powers. Indeed, Lord Bingham himself served as the Interception of Communications Commissioner from 1992 to 1993, although under the statutory framework that preceded the Regulation of Investigatory Powers Act 2000 (RIPA). Among the Bingham Centre's current projects is a review of the law governing the use of intercept material as evidence and on 19 September 2014 the First-Tier Tribunal (Information Rights) upheld the Centre's appeal under the Freedom of Information Act 2000 against the Home Office's refusal to disclose legal advice on this issue.[1] The Centre also held an expert seminar on the investigatory powers review on 1 October 2014 in the London offices of Macfarlanes LLP.

INVESTIGATORY POWERS AND THE RULE OF LAW

4. As a starting point, the Bingham Centre acknowledges that the government has a particular responsibility to protect the public from serious crime, including acts of terrorism.[2] Although this submission does not address "current and future threats to the United Kingdom" (s7(2)(a)), it nonetheless proceeds on the assumption that the United Kingdom will continue to face grave threats to its national security and the safety of its public.

5. On the same basis, the Bingham Centre accepts that the police and intelligence services will - in certain, narrowly-defined and exceptional circumstances - continue to require the power to intercept private communications, access communications data, together with other forms of intrusive surveillance such as the use of covert sources and the power to demand encryption

[1] *Bingham Centre for the Rule of Law v Information Commissioner* [2014] UKFTT 2014/0097 (GRC).

[2] See e.g. the judgment of the European Court of Human Rights in *Öneryildiz v Turkey* (2005) 41 EHRR 20 in which the Grand Chamber held that the right to life under Article 2 ECHR requires governments to "put in place a legislative and administrative framework designed to provide effective deterrence against threats to the right to life" (para 89).

keys. As the European Court of Human Rights held in *Klass v Germany,* "the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[3]

6. The Bingham Centre also recognises that the very effectiveness of covert surveillance depends upon it remaining secret while it is being carried out, and that this secrecy necessarily involves some curtailment of both the right to a fair hearing and the right to an effective remedy of those affected by the surveillance.[4] The necessity of this interference, however, does not mean that the government enjoys an "unlimited discretion" to undertake surveillance.[5] On the contrary, the highly exceptional nature of such powers means that it is all the more important to ensure that the legal framework for investigatory powers complies with the rule of law, including in particular that it must be accessible and sufficiently certain, provide adequate protection for fundamental rights and comply with the United Kingdom's obligations under international law.[6] In our view, these are the benchmarks against which the adequacy of the existing law should be assessed.

THE EXISTING LAW GOVERNING INVESTIGATORY POWERS

7. Although s7(1) DRIPA requires the Home Secretary to appoint the Independent Reviewer "to review the operation and regulation of investigatory powers", the term "investigatory powers" is itself nowhere defined, either in DRIPA, RIPA or elsewhere. On its face, it is an extremely broad term, suggesting any statutory power that may be used by a public body for the purposes of investigation. While in practice it is generally understood as synonymous with "surveillance powers", this only begs the question of how "surveillance" is defined. Even taking a narrow definition of "surveillance", e.g. the *covert* use of statutory powers to collect *private* information about an individual, it is apparent that this would include a great many statutory powers outside either RIPA or DRIPA. For instance:

   (a) Section 94(1) of the Telecommunications Act 1984 allows the Secretary of State to give directions to telecommunications service providers "in the interests of national security or relations with the government of a country or territory outside the United Kingdom";

[3] *Klass v Germany* (1980) 2 EHRR 214 at para 48.

[4] See e.g. *Klass* at para 55: "the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge." See also Lord Neuberger's reference in *In re McE* [2009] UKHL 15 to certain "inherent paradoxical problems" involved in surveillance, one of which is that the authorities "cannot warn the parties in advance that interception or listening in will or will not occur, as to do so would defeat the whole point of the exercise" (para 111).

[5] C.f. *Klass* at para 49: the latitude afforded to domestic legislatures "does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".

[6] See e.g. Tom Bingham, *The Rule of Law* (Penguin, 2010), Part 2, pp37-129.

(b) Part III of the Police Act 1997 provides a framework for authorising interference by police with private property, including the use of surveillance devices;

(c) A number of statutes grant public bodies power to access communications data in certain circumstances, including the Police and Criminal Evidence Act 1984, the Social Security Fraud Act 2001, the Charities Act 1993, the Criminal Justice Act 1987, the Environmental Protection Act 1990, the Financial Services and Markets Act 2000 and the Health and Safety at Work Act 1974;[7]

(d) Section 1(5)(c) RIPA similarly provides for the power of public bodies to intercept stored communications without a warrant by way of "*any statutory power* that is exercised … for the purpose of obtaining information or of taking possession of any document or other property";

(e) Although the Data Retention (EC Directive) Regulations 2009 (SI 2009/859) have now been superseded by Part 1 of DRIPA, the power of the Secretary of State to provide codes of practice for the retention of communications data continues to be set out in Part 11 of the Anti-Terrorism Crime and Security Act 2001.

8. For practical reasons, this submission has focused primarily on those powers contained in RIPA and DRIPA. In our view, however, it is clear that there is a broader need for a coherent and, ideally, comprehensive statutory framework governing the use of covert surveillance powers in general.[8]

Interception of communications

Authorisation

9. The Bingham Centre does not doubt the diligence and conscientiousness of the Secretaries of State in issuing interception warrants nor does it have cause to dispute the candour and integrity

[7] Section 1(6) DRIPA now provides that a public telecommunications operator who retains relevant data under Part 1 of DRIPA must not disclose it except in accordance with an authorisation under Chapter 2 of Part 1 of RIPA, "a court order or other judicial authorisation or warrant" or as provided by regulations made under s1(3) DRIPA.

[8] See e.g. the Report of the Newton Committee of Privy Counsellors on the Anti-Terrorism Crime and Security Act 2001 (HC100, December 2003) at para 406: "we recognise that the need to retain communications data for terrorism and other serious crimes creates the potential for other use or abuse of that data. The protection provided by the Regulation of Investigatory Powers Act is a step in the right direction where it applies, but a coherent legislative framework governing both retention of, and access to, communications data seems to be the only way of providing a comprehensive solution to this issue"; and Lord MacDonald QC, *Review of Counter-Terrorism and Security Powers* (Cm 8003, January 2011) at p7: "although RIPA is the principle legal framework under which communications data may be acquired, there is a wealth of other statutes under which local authorities may also acquire such data. The Review has found that these were mostly not designed with the acquisition of communications data in mind, so that they contain significantly fewer safeguards. This is a very unsatisfactory situation and it needs to be addressed with real urgency if public confidence is to be maintained".

and of those applying for such warrants.[9] We nonetheless consider that it is constitutionally inappropriate for the Secretary of State to have the final say in issuing interception warrants. In their evidence before the Intelligence and Security Committee, the Home Secretary and the Foreign Secretary both stressed the need for democratic accountability in issuing interception warrants, so that government ministers remained answerable for the warrants they issued and could be removed by way of the ballot box if necessary.[10] Yet it is very difficult to see how this could ever be the case. For a start, s17 RIPA prohibits any evidence being adduced in any court or tribunal that would even "tend ... to suggest" that an interception warrant has been made.[11] Secondly, s19 RIPA provides that it is a criminal offence for any person "holding office under the Crown", any member of staff of an intercepting agency or communications service provider, among others, to disclose the existence of an interception warrant unless authorised to do so for certain limited purposes, none of which appear to entail disclosure to Parliament or the public at large.[12]

10. Indeed, in the nearly thirty years since the power to intercept communications has been put on a statutory footing, we are not aware of a single instance in which it was revealed that a government minister signed a particular interception warrant, still less that any minister has ever appeared before Parliament or any court or tribunal or inquiry to account for having done so. In our view, this is because the same secrecy that rightly attaches to the interception of communications by police and intelligence services also prevents meaningful democratic accountability for the Secretary of State's decision to authorise such interception in particular cases.

---

[9] Having said that, we note that concerns have been raised at times; see the remarks of Lord Neuberger in *R(Binyam Mohamed) v Secretary of State for the Foreign and Commonwealth Affairs* [2010] EWCA Civ 65 at para 168, concerning the preparation of public interest immunity certificates: "as the evidence showed, some Security Services officials appear to have a dubious record relating to actual involvement, and frankness about any such involvement, with the mistreatment of Mr Mohamed when he was held at the behest of US officials. I have in mind in particular witness B, but the evidence in this case suggests that it is likely that there were others. The good faith of the Foreign Secretary is not in question, but he prepared the certificates partly, possibly largely, on the basis of information and advice provided by Security Services personnel. Regrettably, but inevitably, this must raise the question whether any statement in the certificates on an issue concerning the mistreatment of Mr Mohamed can be relied on, especially when the issue is whether contemporaneous communications to the Security Services about such mistreatment should be revealed publicly. Not only is there some reason for distrusting such a statement, given that it is based on Security Services' advice and information, because of previous, albeit general, assurances in 2005, but also the Security Services have an interest in the suppression of such information."

[10] "Theresa May's evidence to the intelligence and security committee", by Andrew Sparrow, *The Guardian,* 16 October 2014; "Ministers should assess UK surveillance warrants, says Philip Hammond" by Julian Borger, *The Guardian*, 23 October 2014: "'Perhaps it is a feature of the times that we live in, but I'm sure I can speak for all my colleagues who sign warrants that we all have, in the back of our minds, that at some point in the future we will – not might be, but will – be appearing before some inquiry or tribunal or court to account for the decisions we've made', Hammond said."

[11] Section 18 RIPA provides for certain exceptions to this, yet it is notable that almost all of these relate to courts and tribunals with the power to hold closed proceedings and which are generally under a duty to prevent the disclosure of information contrary to the public interest.

[12] Although s19(9) grants the Interception of Communications Commissioner the power to authorise disclosure, he reports in the first instance to the Prime Minister (s58(4)) who in turn may exclude material contained in the Commissioner's report from being laid before Parliament if he considers that it would be contrary to the public interest for reasons of national security, et al.

11. Moreover, it is generally the case that the Secretary of State who considers an application for a warrant from an intercepting agency is the same person who is accountable to Parliament for its performance, e.g. the Foreign Secretary in the case of MI6 and GCHQ; the Home Secretary in the case of the National Crime Agency, MI5 and the Metropolitan Police; and so forth.[13] There is, therefore, an inevitable risk that, when considering whether to grant an interception warrant, the Secretary of State may give undue weight to broader political considerations at the expense of the fundamental rights of those affected by the surveillance. This risk is especially serious in cases involving the threat of terrorism, and where the rights in question are those of unpopular minorities.[14] In a 2009 case involving directed surveillance of privileged conversations between lawyers and persons in custody, for instance, Lord Neuberger expressed concern at the possibility "that the Government has been knowingly sanctioning illegal surveillance for more than a year".[15] Despite this adverse comment, however, there is no indication that the government faced any public outcry or parliamentary censure as a result of this failing.

12. Even where democratic accountability of surveillance decisions *is* possible (i.e. because authorisations for directed surveillance, unlike interception warrants, may sometimes be disclosed), as the case of *In re McE* shows, the rights of unpopular minorities may be vulnerable where the decision to authorise surveillance is left to the executive. As the ECtHR held in *Klass*:[16]

> *The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.*

---

[13] Save in the case of Scottish warrants for serious crime, s7 RIPA refers only to the power of the Secretary of State to issue warrants and therefore it is exercisable by any of the Secretaries of State: see Schedule 1 of the Interpretation Act 1978. The practice, however, is as outlined above.

[14] See e.g. the judgment of Lord Dyson in *Walumba Lumba v Secretary of State for the Home Department* [2011] UKSC 12 concerning a secret policy operated by the Home Office between 2006 and 2008 concerning the blanket detention of foreign prisoners: "It is material that there is no suggestion that officials acted for ulterior motives or out of malice towards the appellants. Nevertheless, there was a deliberate decision taken at the highest level to conceal the policy that was being applied and to apply a policy which, to put it at its lowest, the Secretary of State and her senior officials knew was vulnerable to legal challenge. For political reasons, it was convenient to take a risk as to the lawfulness of the policy that was being applied and blame the courts if the policy was declared to be unlawful" (para 166).

[15] *In re McE* [2009] UKHL 15 at para 119. At the time of writing, we note also the revelations regarding surveillance of privileged lawyer-client conversations: see *Belhadj & others v Security Service & others*, Case IPT/13/132-9/H, 'Respondents' revised response to claimants' request for further information' 29 October 2014. Documents available in O Bowcott, 'UK intelligence officers spying on lawyers in sensitive security cases', 7 Nov 2014 http://www.theguardian.com/world/2014/nov/06/intelligence-agencies-lawyer-client-abdel-hakim-belhaj-mi5-mi6-gchq.

[16] Para 55. See also e.g. para 56: "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge". The requirement for judicial authorisation is even more explicit in cases involving the seizure of journalistic material under Article 10 ECHR: see e.g. *Sanoma Uitgebers BV and others v Netherlands* (2010) 51 EHRR 31.

13. The Court in *Klass* did not exclude the possibility that effective control could also be exercised by a non-judicial body, so long as it could be shown that it was "independent of the authorities carrying out the surveillance" - i.e. "enjoying sufficient independence to give an objective ruling" - as well as "vested with sufficient powers and competence to exercise an effective and continuous control".[17] In our view, however, it cannot be said that the Secretaries of State are sufficiently independent of the agencies that apply to them for interception warrants; this is because they are accountable to Parliament for the performance of those same agencies.[18] It is *this* aspect of democratic accountability which, in our view, makes government ministers constitutionally ill-suited to grant interception warrants. It is, of course, true that in *Kennedy v United Kingdom,* the Strasbourg Court considered that the Interception of Communications Commissioner and the Investigatory Powers Tribunal provided sufficient judicial control of interception warrants issued by the Secretary of State.[19] For reasons set out in detail below,[20] however, we consider that neither body can properly be said to "exercise an effective and continuous control" over interceptions, and that the ECtHR in *Kennedy* therefore misapprehended the true position under RIPA.

14. Other arguments against judicial authorisation of interception include that it would undermine operational effectiveness,[21] that it would be more resource-intensive than the current model; that it would prevent or inhibit continuing or "downstream" oversight of how interception material is retained and shared. However, these arguments tend to overlook how RIPA *already* provides for judicial authorisation of certain surveillance powers:

    (a) authorisations for police to use intrusive surveillance under Part II must first be approved under s36 RIPA by a Surveillance Commissioner (a person who holds or has held high judicial office under s91(2) of the Police Act 1997);

---

[17] Ibid, para 56.

[18] See e.g. *Kopps v Switzerland* [1999] 27 EHRR 91 at para 74: "It is, to say the least, astonishing that [the] task [of authorising interceptions] should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence".

[19] (2011) 52 EHRR 4 at paras 166-167.

[20] Paras 40-53.

[21] See e.g. the evidence of the then-Interception of Communications Commissioner Sir Swinton Thomas to the Joint Committee on Human Rights: "From a practical point of view, which I suppose is what I am more concerned with, I think it is a very bad idea to put [interception decisions] in the hands of a judge. As things are at the moment, if you know that a bomb has been taken on a train in Leeds and is on its way to King's Cross and you need information, in a matter of minutes you can get a warrant to intercept the communications of that suspected terrorist. Likewise with a serious crime, if a very large consignment of class A drugs has arrived at Dover and is on its way up to Manchester, the Secretary of State is always on duty, 24 hours a day. It is very often absolutely vital that you act with as much speed as you possibly can. That is what currently happens. You can get a warrant or a modification, which is equally important, straight away. Going to a judge would not permit that degree of elasticity. If it is done by a judge, the other side must have the right to be heard and you will not be able to acquire a judicial hearing at the sort of speed that papers can be put in front of the Secretary of State" (12 March 2007, Q26). However, as the then-Director of Public Prosecutions Sir Ken Macdonald QC explained in the same evidence session, there is no reason why judicial authorisation for interception should not be done on an *ex parte* basis (see Q27) and, as Lord Lloyd of Berwick pointed out, there would be no difficulty in getting judicial authorisation "almost as quickly" as with the Secretary of State (Q28).

(b) authorisations for local authorities to access to communications data, use directed surveillance, or covert human intelligence sources must first be approved by a magistrate under ss23A-D RIPA (as amended by ss37-38 of the Protection of Freedoms Act 2012); and

(c) permission to make an encryption notice under Part III must be given by a Circuit judge under paragraph 1(1) of Schedule 2 RIPA.[22]

15. Of these, we consider that the work of the Surveillance Commissioners in approving the use of intrusive surveillance by police provides a useful model for judicial authorisation of interception warrants under RIPA for the following reasons:

(i) it is well-known that intrusive surveillance may enable police to access the contents of private communications almost as readily as interception (e.g. recording a telephone conversation by way of a covert listening device or viewing a computer screen by way of a hidden camera);[23]

(ii) the Surveillance Commissioners are already obliged to consider the likelihood that the use of intrusive surveillance may result in the acquisition of legally privileged material (as well as the likelihood of obtaining "confidential information" under the Police Act 1997, including not only privileged material but also confidential journalistic material, personal information, or communications with an MP on constituency matters);[24]

(iii) s36(2) RIPA provides for police to use intrusive surveillance without judicial approval in cases of urgency, subject to subsequent review by a Surveillance Commissioner who has the power to quash or cancel such authorisations under s37(2) or (3). (We note, moreover, that this is consistent with the procedures in most countries which require judicial authorisation for interception, in that they allow for emergency self-authorisation by police subject to judicial confirmation within 24 or 48 hours);[25]

(iv) in addition to approving the use of intrusive surveillance by police, the Surveillance Commissioners also provide "downstream" oversight by way of their role in reviewing the renewal of authorisations as well as by way of the annual report of the Chief

[22] Save where the police or intelligence services have obtained the encrypted material by way of a warrant made by the Secretary of State: see paragraph 2 of Schedule 2 RIPA.

[23] See e.g. *R v Allsop and others* [2005] EWCA Crim 703; *R v E* [2004] EWCA Crim 1243; *R v Smart and another* [2002] EWCA Crim 772.

[24] In her evidence to the Intelligence and Security Committee in October 2014, the Home Secretary suggested that a key difference between judicial authorisation of search warrants and that of interception warrants was that a search takes place in public whereas surveillance involves a different kind of intrusion. In our view, however, the different nature of the intrusion only makes judicial authorisation *more* necessary. More to the point, intrusive surveillance by the police under Part II RIPA also involves considerable secrecy, yet it is not suggested that judicial authorisation in these cases is somehow less appropriate.

[25] See e.g. 18 US Code § 2518(7), enabling interception without a judge's order where there is immediate danger of death or serious physical injury, or "conspiratorial activities" which either threaten national security or are characteristic of organized crime, so long as an application is made to a judge within 48 hours.

Commissioner under s62 RIPA. Again, this is consistent with the procedure of other jurisdictions which require judicial authorisation;[26]

(v) the Surveillance Commissioners have each held high judicial office, which means that they are each former Court of Appeal or High Court judges or their Scottish equivalent.

16. We do not suggest that it is the Surveillance Commissioners themselves who should necessarily assume responsibility for making interception warrants: in our view, the same function could in principle also be carried out by any High Court judge (see e.g. their expertise in cases involving terrorist asset-freezing, TPIMs and deportation on grounds of national security) or even the specialist district court judges who preside over cases involving extradition or terrorism. If judicial supervision is possible in these areas involving highly sensitive matters of national security and close scrutiny of the activities of the intelligence services, then it should also be possible in the case of interception of communications. In any event, the role of the Surveillance Commissioners shows not only how judicial authorisation of surveillance powers *may* work in practice, but also that it *has* worked for nearly fifteen years under Part II of RIPA.[27]

17. For the avoidance of doubt, we do not recommend that the judge's task be confined to deciding whether or not to *approve* an authorisation – rather, the relevant agency should apply for an interception warrant in the same manner as a search warrant, i.e. it is for the judge himself or herself to decide whether the surveillance sought is necessary and proportionate, rather than simply reviewing whether the applicant's assessment of necessity and proportionality was reasonable. We also recommend that the judge should have the power to direct the appointment of a special advocate in appropriate cases (e.g. where the application is particularly complex) in order to test the application in a closed hearing, just as a judge may currently do in cases involving public interest immunity[28] and is routinely the case in applications for surveillance in Queensland, Australia.[29]

Bulk interception of 'external' communications under s8(4)

18. At the time of writing, the legality of warrants for the bulk interception of external communications under s8(4) RIPA is the subject of several legal challenges, before both the

[26] See e.g. 18 US Code § 2518(6), under which an interception order "may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception".

[27] Moreover, if it is correct that the Home Secretary spends a "significant part of her day dealing with intercept and surveillance warrants",(see "Theresa May defends culture of secrecy over mass snooping" by Alan Travis, The Guardian, 16 October 2014) then it is apparent that an additional benefit of judicial authorisation is that it would enable each of the relevant Secretaries of State to devote more time to those duties to which they are constitutionally better-suited to discharge.

[28] See *R v H* [2004] UKHL 3 at para 36.

[29] See the role of the Public Interest Monitor under s326(b) of the Crime and Misconduct Act 2001 (Qld) as set out in JUSTICE, *Secret Evidence* (June 2009) at paras 333-337.

Investigatory Powers Tribunal[30] and the European Court of Human Rights.[31] In outline, the key issues are as follows:

(a) unlike a warrant issued under s8(1), there is no requirement for a warrant under s8(4) to be targeted at the communications of either a particular person or a specific premises. As the Investigatory Powers Tribunal noted in *British Irish Rights Watch and others v Security Service and others*, a warrant under s8(4) may in principle result in "the interception of all communications between the United Kingdom and an identified city or country".[32] The only constraint is what the Secretary of State considers to be necessary in the interests of national security, the detection or prevention of serious crime, safeguarding the economic well-being of the United Kingdom,[33] or for the purposes of giving effect to an international mutual legal assistance agreement (s5(3) RIPA);

(b) although a warrant under s8(4) only authorises the interception of "external" communications (defined by s20 as those either sent or received outside the British Islands), s5(6) RIPA further authorises the interception of any such communications not identified by the warrant as is necessary in order to intercept the external communications in question. As Lord Bassam told Parliament in 2000, "it is just not possible to ensure that only external communications are intercepted" and "there is no way of filtering ... out [internal] communications without intercepting the whole link".[34] In practical terms, therefore, the interception of external communications is liable to involve the interception of an unknown number of internal communications as well;

(c) although Parliament was told in 2000 that email sent and received within the UK would not fall within the definition of "external communications" under s20, even if it was routed outside the UK in transit,[35] it remains unclear how this definition would apply to such activities as an inquiry made of a search engine or a post to a friend's page using social media. It was not until 16 May 2014 that a senior Home Office official revealed in a witness statement that the intelligence services considered that search engine inquiries and posts to social media platforms were "external communications" for the purposes of s8(4) RIPA, so long as the relevant server was outside the British Islands, notwithstanding that the only persons involved in the communication were within the UK at all material times;[36]

---

[30] See *Liberty, the ACLU and others v GCHQ and others* (IPT/13/77H, IPT/13/168-173/H); *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (IPT/13/92/CH); and *Amnesty International v The Security Service and others* (IPT/13/194/CH).

[31] See *Big Brother Watch and others v United Kingdom* (no 58170/13, lodged 4 September 2013).

[32] IPT/01/77, 9 December 2004 at para 9.

[33] This ground has now been narrowed by s3 DRIPA to only those economic interests that are "also relevant to the interests of national security". In addition, s5(5) RIPA has always provided that a warrant cannot be necessary for the purposes of safeguarding economic interests unless the information in question relates "to the acts or intentions of persons outside the British Islands"

[34] Hansard, HL debates, 12 July 2000, col 323.

[35] See the speech of Lord Bassam, ibid and para 5.1 of the Interception of Communications Code of Practice, issued in July 2002 under s71 RIPA.

[36] See witness statement of Charles Farr dated 16 May 2014 at paras 132-138.

(d) the primary safeguard to prevent internal communications collected under s8(4) warrants being "read, looked at or listened to" by the intelligence services is that set out under s16(2), which prohibits officials from selecting material for inspection by reference to a factor which is "referable to an individual who is known to be for the time being in the British Islands", where one of the purposes of the search is to identify "material contained in communications sent by him or intended for him". There is nothing in s16 or elsewhere in RIPA, however, to prevent a person's internal communications being searched by reference to *other* factors which may nonetheless lead to disclosure of his or her sensitive personal information, e.g. religious beliefs, medical status, sexual orientation or political opinions;

(e) on the same basis, there is nothing under s16 or elsewhere in RIPA to prevent the *data* related to internal communications intercepted under s8(4) - e.g. traffic data, subscriber data and service use data - being collected, retained and used by the intelligence services for whatever purpose they consider to be necessary for the purposes of national security, etc under s5(3). To the extent that there is any internal guidance that further restricts how internal communications and related data may be used, the intelligence services have refused to disclose this on the grounds that it would be prejudicial to national security.

19. In the Bingham Centre's view, the current framework governing the bulk interception of communications and related data under s8(4) raises a number of concerns.[37] First, the relevant provisions - especially the definition of "external communication" under s20 - appear to us to lack sufficient clarity and certainty to comply with the fundamental requirements of the rule of law.[38] Secondly, we doubt whether the location from which a particular communication was sent or received (i.e. within or without the British Islands) provides a sufficient basis on which to distinguish between the narrow and targeted requirements of warrants under s8(1) with the virtually unrestrained breadth of warrants under s8(4). Thirdly, the practice of bulk interception - in which potentially millions of internal communications may be intercepted for the sake of obtaining a particular external communication - seems to us to be fundamentally at odds with the very concept of proportionality itself. In our view, all warrants and authorisations must be

[37] For reasons of space, we are unable to address an equally pressing issue which is the extent to which the intelligence services may *receive* communications data and the contents of communications collected by foreign intelligence agencies.

[38] C.f.. *Liberty and others v United Kingdom* (2009) 48 EHRR 1 at para 69, in which the ECtHR held that the relevant provisions of the Interception of Communications Act 1984 breached Article 8 ECHR because, inter alia, they did not "indicate with sufficient clarity ... the scope or manner of the very wide discretion conferred on the State to intercept and examine external communications ... In particular it did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material"; see also *Weber and Saravia v Germany* (2008) 46 EHRR SE5 at para 94: the law governing interception must "indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference".

founded on the reasonable suspicion of the authorities that a particular individual has been involved in serious criminal activity (which would, of necessity, include terrorist offences).

20. Nor is the scale of the apparent interference with the right to privacy mitigated by the fact that relatively few of the communications intercepted by the intelligence services under a s8(4) warrant may be "read, looked at or listened to" under s16(2). In this context, we note the recent judgment of the CJEU in *Digital Rights Ireland*, in which the Grand Chamber held that the blanket retention of customers' communications data for up to 2 years under the 2006 Data Retention Directive entailed "an interference with the fundamental rights of practically the entire European population" contrary to the rights to privacy and data protection under Articles 7 and 8 of the EU Charter of Fundamental Rights because it did "not require any relationship between the data whose retention is provided for and a threat to public security".[39]

21. For these reasons, we recommend that the current power to intercept external communications under s8(4) be repealed. At the very least it should be severely curtailed. We note that there is no statutory restriction against using s8(1) warrants in respect of so-called "external" communications. We see no reason, therefore, why targeted warrants should not be used in respect of external communications on the same basis that they are used within the UK.

Intercept as evidence

22. Section 17(1)(a) RIPA prohibits the use of intercept obtained under warrant as evidence in either criminal or civil proceedings.[40] In January 2008, a review committee of Privy Counsellors reported its conclusion that "intercept as evidence should be introduced", subject to certain operational tests that would have to be met.[41] In December 2009, the Home Secretary reported to Parliament that it had been unable to produce a viable model that met the legal requirements identified by the Privy Council.[42] The Home Secretary nonetheless stated that the Home Office's implementation team would continue to work to "identify a way forward".[43] As recently as June 2013, a Home Office minister told Parliament that the government was continuing to review the use of intercept as evidence, "under the guidance of the cross-party group of Privy Counsellors" and that it would "report back to the House in due course".[44] As of yet, there has been no subsequent report.

23. In our view, intercept evidence is one of the most compelling and probative forms of evidence available.[45] It is widely used in other common jurisdictions with similar criminal and civil

[39] *Digital Rights Ireland v Minister for Communications and others* (2014) ECLI:EU:C:2014:238 at paras 56 and 59.
[40] Notably, evidence obtained by way of interception without a warrant under ss3 or 4 RIPA (e.g. interceptions in prisons, etc) *are* admissible.
[41] Cm 7324, at para 204.
[42] Cm 7760 at paras 23-25.
[43] Ibid, para 25.
[44] 6 June 2013, col 1229W.
[45] As Lord Lloyd of Berwick told Parliament during the debates on what became s17: "We have here a valuable source of evidence to convict criminals. It is especially valuable for convicting terrorist offenders

proceedings as our own,[46] including some with more onerous requirements governing the disclosure of relevant unused material.[47] And, as Lord Bingham noted in 2004, there is nothing in the ECHR that prohibits the use of intercept as evidence.[48] On the other hand, the lack of provision for intercept evidence has not only made it more difficult to prosecute terrorism offences, but increased resort to exceptional measures such as TPIMs.[49] We therefore consider it essential that any reform of the legal framework of investigatory powers in the UK must address the issue of intercept evidence.

Communications data

The changing nature of communications data

24. The lower level of protection accorded to communications data under Chapter 2 of Part 1 of RIPA reflects the longstanding view that the content of any given communication is necessarily more sensitive than the data which relates to it. In the 1984 case of *Malone v United Kingdom*,

---

because in cases involving terrorist crime it is very difficult to get any other evidence which can be adduced in court, for reasons with which we are all familiar. We know who the terrorists are, but we exclude the only evidence which has any chance of getting them convicted; and we are the only country in the world to do so" (Hansard, HL Debates 19 June 2000, col 109-110); see also the views of the Joint Committee on Human Rights, *Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning*, HL 157/HC 394, 16 July 2007 at para 126: "We are satisfied that the evidence of the DPP and the former Attorney General puts the matter beyond doubt: that the ability to use intercept as evidence would be of enormous benefit in bringing prosecutions against terrorists in circumstances where prosecutions cannot currently be brought, and that the current prohibition is the single biggest obstacle to bringing more prosecutions for terrorism. We recommend that this be taken as the premise of the forthcoming review by the Privy Council. The difficult question is not whether the current ban on the evidential use of intercept should be relaxed, but how to overcome the practical obstacles to such a relaxation".

[46] See e.g. *Intercept Evidence: Lifting the Ban* (JUSTICE, October 2007).

[47] See e.g. "The Unique Challenges of Terrorism Prosecutions" (Ch 7) vol 4 at p267), *Air India Flight 192: A Canadian Tragedy* (June 2010): "In general, disclosure obligations in both the United States and the United Kingdom are less broad than in Canada. Both the United States and the United Kingdom attempt to flesh-out disclosure requirements in statutes and other rules while, as discussed above, Canada relies on a case-by-case adjudication under the Charter. Both the decreased breadth and increased certainty of disclosure requirements in the United States and the United Kingdom may make it less necessary for prosecutors to claim national security confidentiality over material that may be relevant to a case, but which does not significantly weaken the prosecution's case or strengthen the accused's case."

[48] *Attorney General's Reference No 5 of* 2002 [2004] UKHL 40 at para 14: "the United Kingdom practice has been to exclude the product of warranted interception from the public domain and thus to preclude its use as evidence. But this has been a policy choice, not a requirement compelled by the Convention, and other countries have made a different policy choice. Article 8(2) of the European Convention permits necessary and proportionate interference with the right guaranteed in Article 8(1) if in accordance with the law and if in the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. Save where necessary to preserve the security of warranted interception, there is no reason why it should have been sought to exclude the product of any lawful interception where relevant as evidence in any case whether civil or criminal".

[49] See e.g. Home Office Minister Lord Rooker, Hansard, HL Debates, 27 November 2001, col 146: "If we could prosecute on the basis of the available evidence in open court, we would do so. *There are circumstances in which we simply cannot do that because we do not use intercept evidence in our courts*".

[50] for instance, the British government had argued that the practice of 'metering' (which involved a meter check printer being attached covertly to a telephone line to record "the numbers dialled on a particular telephone and the time and duration of each call")[51] did not entail any interference with the applicant's rights under Article 8 ECHR. Although this argument was rejected by the ECtHR on the basis that the relevant data was "an integral element in the communication", it accepted that the collection of data was nonetheless to be distinguished from the interception of content.[52]

25. It is obvious, however, that there has been a fundamental shift in the nature of communications technology over the past three decades. Not only is there increasing convergence of communications *networks* (e.g. voice and data being carried on the same infrastructure) but also a convergence of *functions*, so that most individuals now carry at least one or more devices which are each capable of communicating in a number of different ways, e.g. a person who uses his or her mobile phone to make calls, send texts and emails, post on social media and browse websites on the Internet.

26. In addition to the fact that most of our private communications are now made via the Internet, it is also apparent that there has been a vast increase in the amount of communications data that is generated by each person, which is then automatically collected and stored by a wide range of communications service providers and accessible to public authorities under RIPA. It is apparent that the analysis of such data – including not only numbers dialled and the time and duration of a call but also geo-location data and the IP addresses of websites visited – can readily disclose details of a person's relationships with others as well as various patterns of behaviour capable of revealing broad range of sensitive information about that individual, including their ethnic origin, their political opinions or religious beliefs, their physical or mental health, and/or their sexual orientation.[53]

27. In our view, it is clear that there is very little meaningful comparison between the quality of information available from the Post Office's metering of a single landline in the early 1980s and that available from an ordinary mobile phone more than three decades later. The idea that

[50] (1984) 7 EHRR 14.
[51] Ibid, para 83.
[52] Para 84.
[53] For example, a study by the Center for Internet and Society at Stanford Law School analysed the communications data gathered from 546 mobile phone users ("MetaPhone: The Sensitivity of Telephone Metadata" by Patrick Mutchler and Jonathan Mayer, 12 March 2014). In the first instance, it noted that, in certain cases, the simple fact that a number was called was itself highly sensitive in nature: "Participants had calls with Alcoholics Anonymous, gun stores, NARAL Pro-Choice, labor unions, divorce lawyers, sexually transmitted disease clinics, a Canadian import pharmacy, strip clubs, and much more". The study went on to find "a number of patterns that were highly indicative of sensitive activities or traits", for example: "Participant A communicated with multiple local neurology groups, a specialty pharmacy, a rare condition management service, and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis" and "Participant E had a long, early morning call with her sister. Two days later, she placed a series of calls to the local Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after".

intercepting the content of a person's communications is always more intrusive than accessing their communications data is simply no longer sustainable. The interception of the content of any particular telephone call by an individual may reveal very little about that person's religious beliefs, their medical information or their sexual orientation. Access to and analysis of the communications data from the same person's mobile phone may, by contrast, readily disclose a wealth of highly sensitive information about that person, all without a single word of their communications being read, looked at or listened to by anyone else. By the same token, it is equally true that access to communications data may also disclose information subject to legal professional privilege or the identity of a journalist's source. We are concerned, therefore, by recent revelations that the Metropolitan police may have been using authorisations under Chapter 2 to access communications data as a means of avoiding the requirements of the Police and Criminal Evidence Act 1984 in respect of journalistic material.[54]

Authorisation

28. Given the obvious sensitivity of communications data, it is clear that existing procedures for authorising access to such data are inadequate. In the first instance, Chapter 2 of Part 1 of RIPA provides that when a public body seeks access to communications data, the person responsible for authorising the request is, in almost every case, a senior member of the same agency. Even if senior officials scrutinize applications for communications data with great care, it is plain that they are not independent of the agency carrying out the surveillance and are therefore institutionally incapable of the objectivity needed to give an impartial decision on the merits of the application.

29. In this respect, we note that Protection of Freedoms Act 2012 introduced a requirement for prior judicial authorisation of communications data requests by local authorities, together with a power for the Secretary of State to extend this requirement to other public bodies by way of an order. While this might at first glance appear to provide an appropriate way forward, we note that serious concerns have been expressed that many magistrates do not have sufficient training or expertise to provide the necessary degree of supervision.[55] We therefore recommend that authorisation for access to communications data should be placed on the same footing as the interception of communications: i.e. ideally authorised High Court judges or their equivalent. Similarly, in cases of urgency, the police and intelligence services should have the power to self-

[54] See, for example, 'A Travis, 'Police told to reveal the use of surveillance powers to identify journalists' sources', *The Guardian*, 6 Oct 2014, http://www.theguardian.com/uk-news/2014/oct/06/police-ordered-reveal-ripa-powers-identify-journalists-sources. We welcome the government's undertaking to reform the law: P Wintour, 'British police's use of Ripa powers to snoop on journalists to be reined in' *The Observer*, 12 Oct 2014, http://www.theguardian.com/world/2014/oct/12/police-ripa-powers-journalists-surveillance.

[55] See e.g. the 2014 report of the Chief Surveillance Commissioner at para 3.10: "What has become clear is that the knowledge and understanding of RIPA among magistrates and their staff varies widely. Adequate training of magistrates is a matter for others, but I highlight the need. The public is not well served if, through lack of experience or training, magistrates are not equipped effectively to exercise the oversight responsibility which the legislation requires. I am aware, for example, of one magistrate having granted an approval for activity retrospectively, and another having signed a formal notice despite it having been erroneously completed by the applicant with details of a different case altogether."

authorise access to communications data so long as it is subject to judicial confirmation within 48 hours.

30. A separate concern is that, unlike interception warrants under s8(1), there is no requirement that a request for access to communications data be targeted against a particular individual. We therefore recommend that this requirement be introduced to ensure that the power to access communications data is not exercised disproportionately.

31. More generally, we recommend that both the number of statutory powers to access communications data and the number of public bodies able to wield those powers should be severely curtailed. In the latter case, we recommend that the power to access such data should be restricted to the police, the intelligence services and the limited number of other public bodies with a responsibility to investigate serious criminal activity.[56] As regards the former, we note that the current government has already committed itself to ensuring that "RIPA is the only mechanism by which communications data can be acquired"[57] and we further note the requirement in s1(6) DRIPA prohibiting disclosure of communications data retained by a public telecommunications operator pursuant to a retention notice other than by way of Chapter 2 RIPA or "a court order or other judicial authorisation or warrant" or under regulations made by the Secretary of State. Although this is a welcome move, we note that it does not prevent access to communications data held by *other* communications service providers otherwise than pursuant to a retention notice, nor has the Secretary of State published any regulations in draft.

Intrusive surveillance, directed surveillance and covert sources

32. The distinction under Part 2 RIPA between 'intrusive' and 'directed' surveillance is meant in principle to ensure that any surveillance that is likely to involve a serious interference with a person's privacy (i.e. intrusive) requires a much higher level of authorisation than those which do not (i.e. directed). However, as the Code of Practice itself notes, the statutory definition of 'intrusive' "relates to the *location* of the surveillance [i.e. within a person's home or vehicle] and *not* any other consideration of the nature of the information that is expected to be obtained". It is therefore not necessary, the Code continues, "to consider whether or not intrusive surveillance is likely to result in the obtaining of private information".[58] Part 3 of the Police Act 1997, by contrast, requires judicial authorisation whenever property interference is likely to result in "the acquisition of knowledge of matters subject to legal privilege, confidential personal information or confidential journalistic information".[59]

---

[56] C.f. the 2009 recommendation of the House of Lords Constitution Committee that "such powers should only be available for the investigation of serious criminal offences which would attract a custodial sentence of at least two years" (*Surveillance, Citizens and the State*, HL 18, January 2009, para 177). An exception could also be made for the other emergency services who sometimes need to access subscriber data in order to identify persons involved in accidents, etc.

[57] Home Office Review of Counter-Terrorism Powers (Cm 8004, January 2011), p 29.

[58] Para 2.11.

[59] Ibid, para 4.12.

33. The possibility that 'directed' surveillance may prove highly intrusive was highlighted in *In re C*, in which the Divisional Court in Northern Ireland held that the use of surveillance to monitor privileged communications between lawyers and suspects in prison cells and custody suites was unlawful because of the lack of prior judicial authorisation.[60] However, although the subsequent 2010 order[61] introduced the requirement for such authorisation in order to monitor 'legal consultations' in places of detention, it is notable that it still adopted a location-based approach rather than one of substance. In other words, it is still permissible under RIPA to use directed surveillance of a privileged conversation that takes place in a town hall or an MPs office or a park bench, etc.

34. We therefore recommend that the definition of 'intrusive' surveillance be tightened, so that the former includes *any* covert surveillance that either involves or is likely to involve a significant interference with a person's privacy. 'Directed' surveillance, in contrast, would be any use of covert surveillance that either does not or is not likely to involve a significant interference with a person's privacy.

35. For the same reasons outlined above in respect of interception and communications data, we also recommend that the power of the Secretary of State to authorise intrusive intelligence by the intelligence services under s41 RIPA should be repealed. Instead, *all* use of intrusive surveillance should be authorised by the Surveillance Commissioners or a judge of equivalent level.

36. As regards the use of covert sources, we note an increasing number of revelations in recent years concerning the conduct of undercover officers, including in particular members of the National Public Order Intelligence Unit, the National Domestic Extremism Unit, and the Metropolitan Police's Special Demonstration Squad. These have resulted not only in a series of investigations by HM Inspector of Constabulary, the National Crime Agency and the Independent Police Complaints Commission among others, but also several miscarriages of justice[62] and, in the most recent case, a settlement of £425,000 to a woman whose child was fathered by an undercover police officer.[63]

37. In our view, these cases further highlight the inadequacy of the internal self-authorisation model that underpins much of RIPA. We note, moreover, the 2011 recommendation of the then-President of the Association of Chief Police Officers, Sir Hugh Orde, that judicial authorisation

[60] [2007] NIQB 101, subsequently upheld by the House of Lords in *In re McE* [2009] UKHL 15.
[61] The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010 (SI 2010/461).
[62] *David Robert Barkshire and others v The Queen* (Court of Appeal Criminal Division, unreported, 20 July 2011).
[63] See e.g. BBC News, "Met pays £425,000 to mother of undercover policeman's child", 24 October 2014.

of undercover officers should be required in complex cases.[64] The Chief Surveillance Commissioner has also indicated that he was "also agreeable in principle to Commissioners giving prior approval to certain kinds of such activity by a [covert human intelligence source], provided that the OSC is given the appropriate resources to deal with the number of cases which arise and subject to any necessary legislation conferring the power".[65] We therefore recommend that the use of undercover officers should be authorised by a judge in any case where their conduct is likely to involve a significant interference with another person's privacy.

Encryption keys

38. The threat of terrorism has since the 1990s been cited by government officials as justifying the need for a statutory power to obtain encryption keys,[66] though the powers under Part 3 of RIPA were not brought into force until October 2007. Since then, it does not appear to have been widely used by either the police or the intelligence services and, when it has been used, it has mostly been used for non-terrorist offences such as child sex abuse.[67]

39. Although we consider that the power to obtain encryption keys is, in certain circumstances, a necessary one, there are a number of ways that the existing framework could be improved. First, Part 3 of RIPA is poorly-drafted. As we noted above, accessibility and certainty are both core requirements of the rule of law and the ECtHR has repeatedly made clear the need for "clear, detailed rules" and "accessibility and clarity" not only in the case of interception but also to "more general programmes of surveillance".[68] Secondly, permission to make a notice can only be made by a Circuit Judge, save where the encrypted material has been obtained under a warrant from or with the authorisation of the Secretary of State.[69] As with interception, communications data, and intrusive surveillance, we recommend that the Secretary of State should play no role in authorising surveillance. Instead, an encryption notice should only be authorised by a judge.[70] Thirdly, although there has already been some judicial consideration of the privilege against self-incrimination,[71] neither RIPA nor the Code of Practice make any allowance for journalistic material or material covered by legal professional privilege corresponding with the safeguards contained in PACE.

---

[64] Sir Hugh Orde, "Undercover Policing and Public Trust", 7 February 2011.
[65] 2011-2012 report, para 5.1.
[66] See e.g. Department of Trade and Industry, Paper of Regulatory Intent concerning Use of Encryption on Public Networks (June 1996).
[67] See e.g. the report of the Chief Surveillance Commissioner for 2009-2010 at para 4.11: "[The offence of] the possession of indecent images of children … is the main reason why section 49 notices are served. Other offences include: insider dealing, illegal broadcasting, theft, evasion of excise duty and aggravated burglary. It is of note that only one notice was served in relation to terrorism offences". See more generally JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (October 2011), paras 327-333.
[68] *Liberty and others v United Kingdom* (2009) 48 EHRR 1 at para 63.
[69] Paragraph 2 of Schedule 1 of RIPA.
[70] In cases involving the intelligence services and other sensitive cases, it may be more appropriate for the application to be made to a security-cleared High Court or Crown Court judge rather than a Circuit Court judge.
[71] See *R v S and A* [2008] EWCA Crim 2177 and *Greater Manchester Police v Andrews* [2011] EWHC 1966 (Admin).

Oversight

The Commissioners

40. In *Kennedy*, the ECtHR described the Interception of Communication's review of "a random selection of specific cases in which interception has been authorised" as "an important control of the activities of the intercepting agencies and of the Secretary of State himself".[72] The Bingham Centre agrees that the oversight provided by the Interception Commissioner - together with that provided by the Intelligence Services Commissioner and the Chief Surveillance Commissioner – constitutes an extremely important safeguard against the unnecessary or disproportionate use of surveillance powers. As valuable as this independent safeguard is, however, we consider that the oversight regime provided by the Commissioners suffers from a number of significant deficiencies.

41. First, it is clear that the remit of each Commissioner, taken together, does not provide comprehensive oversight of the exercise of surveillance powers under RIPA. The Interception of Communications, for instance, has no statutory remit in respect of interceptions under section 3 and has only agreed to provide oversight of interceptions in prisons on a "non-statutory" basis.[73] This does not, however, include other places of detention such as private prisons or secure mental health facilities, nor does it extend to the very broad power of communications service providers and operators of private communications networks to intercept communications for "the purposes connected with the provision or operation of a [telecommunications] service" under ss 3(1) and 3(3) respectively.

42. Secondly, the current framework defines the remit of each oversight Commissioner according to function in some cases and by agency in other cases. In practical terms, this means that surveillance of a privileged communication between a suspected terrorist and his lawyer may be subject to oversight by three different Commissioners, depending entirely on how it was authorised and according to which agency carried out the surveillance, i.e.:

    a. If the phone conversation was intercepted under Part 1 RIPA then the Secretary of State's warrant would be subject to review by the Interception of Communications Commissioner;

    b. If the phone conversation was monitored by way of a hidden microphone planted in the suspect's home by one of the intelligence services, then the Secretary of State's authorisation for intrusive surveillance under Part 2 RIPA would be subject to review by the Intelligence Services Commissioner; or

[72] *Kennedy*, para 166.

[73] See the 2002 report of Sir Swinton Thomas at para 59: 'I have been asked by the Home Office, and have agreed in principle, to oversee the interception of communications in prisons'.

c. If the phone conversation was monitored by way of a hidden microphone planted in the suspect's home by the police, then review of the authorisation for intrusive surveillance under Part 2 RIPA would be subject to review by the Chief Surveillance Commissioner.

The potential for this piecemeal oversight also arises in other parts of RIPA: e.g. the use of encryption notices under Part 3 which has been reported on by all three commissioners. In our view, it is highly undesirable that the same intrusion could be subject to oversight by three different bodies, each with their own distinct procedure and approach, depending on the choice of methods and the agency involved.

43. Thirdly, it is apparent that both the Interception of Communications Commissioner and the Intelligence Services Commissioner are part-time posts, and inspect only a small sample of the warrants and authorisations made annually under Part 1 RIPA by the various Secretaries of State.[74] In his most recent report, for instance, the Interception of Communications Commissioner stated that he inspected approximately 600 applications for warrants made in 2013,[75] amounting to little more than 20% of the 2760 warrants issued that year. Although the Commissioner has defended this as a "sufficient representative sample of the individual warrants",[76] we note that each warrant embodies a decision by a member of the executive to invade the privacy of one or more persons (and in the case of a warrant under s8(4), potentially millions of people). It is therefore not acceptable, in our view, that approximately 4 in every 5 warrants, and more than 90% of authorisations to access communications data, are never looked at by a judge, even after the fact.

44. Fourthly, even when warrants and authorisations are scrutinized, it remains unclear what standard is applied by the reviewing Commissioner in each case, e.g. does he satisfy himself whether the interference with Article 8(2) was necessary and proportionate[77] or does he simply consider whether the Secretary of State's assessment of those factors was *Wednesbury* reasonable?

45. Fifthly, even in the unlikely event that the Interception of Communications Commissioner discovered that the Secretary of State had made a warrant that he considered to be unlawful, RIPA does not provide him with any power to quash the warrant. He may, of course, report the matter to the Prime Minister under s58(2) but the Prime Minister has the discretion to redact such information from the report laid before Parliament. Nor does the Interception of

[74] House of Commons Home Affairs Committee, *Counter-terrorism* (HC 231, April 2014) at para 163: "The information given to us by the Commissioners indicate that they examine a small number of warrants under the current oversight system. The Intelligence Services Commissioner told us that in 2012 he had examined 8.5% of warrants. The Interception of Communications Commissioner told us that he had examined between 5% and 10% of the applications. He was not able to be more specific as he did not know how many applications there were."
[75] Para 3.36.
[76] Para 3.37.
[77] c.f. *Huang v Secretary of State for the Home Department* [2007] UKHL 11 at para 20.

Communications Commissioner have the power to refer a possible breach of Article 8 ECHR to the Investigatory Powers Tribunal.

46. For the above reasons, the Bingham Centre does not consider that the Commissioners overall provide "effective control" of surveillance powers under RIPA, save in the limited circumstances where those powers have already been subject to prior judicial authorisation (e.g. the use of intrusive surveillance where approved by the Surveillance Commissioners, or the use of directed surveillance by local authorities). In our view, extending judicial authorisation across the board would go a long way to reducing the administrative burden on the commissioners. While the burden will, of course, shift rather than disappear, the shift is worthwhile as it is of vital importance for control to be effective. Even so, it is apparent that the different oversight schemes are in need of rationalisation and we therefore recommend that the current functions be combined within a single, properly-staffed and funded body providing more coherent and effective oversight. We also recommend that this body have a broader remit to oversee the use of *all* surveillance powers by public bodies, rather than the current fragmented statutory regime. Although concerns have been expressed that putting oversight on a more permanent footing may result in less independent-minded candidates being available, we consider that it should be possible to devise a model that strikes an appropriate balance between independence and effectiveness. We note, for instance, that the Law Commission is chaired by a High Court or Appeal Court judge, serving for up to three years. We see no reason why appointment to chair the statutory oversight regime for surveillance powers should not be on a similar footing.

Investigatory Powers Tribunal

47. Just as the ECtHR in *Kennedy* praised the role of the oversight Commissioners, so too it commended the Investigatory Powers Tribunal as an "independent and impartial body, with its own rules of procedure" that constituted a "general safeguard" against the abuse of surveillance powers.[78] In addition, the ECtHR found that the procedures of the Tribunal did not "impair the very essence of the applicant's Article 6 rights", notwithstanding that the Tribunal considered his specific complaints in private without him being present, did not provide the applicant with any disclosure, did not afford him the opportunity to cross-examine any witnesses on the other side, and did not appoint a special advocate to represent his interests in any of the hearings from which he had been excluded.[79]

48. In our view, however, the decision of the ECtHR in *Kennedy* is not consistent with its own established jurisprudence on the justiciability of surveillance decisions under Article 6.[80] More

[78] See *Kennedy*, paras 167 and 169.
[79] Ibid, para 184-190.
[80] See e.g. *Klass* at para 75: "the question whether the decisions authorising such surveillance under the [German statute] are covered by the judicial guarantee set forth in Article 6…must be examined by drawing a distinction between two stages: that before, and that after, notification of the termination of surveillance. As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned, within the meaning of Article 6 … as a consequence, it of necessity escapes the requirements of that Article"; see also the dissent of Lord Kerr in

generally, while we accept that the Tribunal constitutes an essential safeguard against unlawful and disproportionate surveillance,[81] we are concerned that it is also severely flawed in a number of respects.

49. First, the proportion of applicants who are successful in their complaints before the Tribunal is extremely low – some 0.5% in the first decade of its operation.[82] In contrast, the annual success rate for complainants before other tribunals varies between 13% (mental health) and 41% (immigration and asylum).[83] In our view, the very poor success rate of complaints before the IPT does not necessarily reflect the quality of decision-making in the field of surveillance powers but rather almost certainly reflects the difficulty of bringing an effective challenge against the use of covert powers in a Tribunal in the absence of (i) proper notification requirements and (ii) any right to disclosure.

50. In *Klass*, the ECtHR conceded that the lack of any requirement on a public body to notify a person that they had been subject to surveillance following its conclusion meant that there was "in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality".[84] Despite this, the Strasbourg Court held that, although desirable, the absence of notification of surveillance did not breach the right to an effective remedy under Article 13 ECHR.[85] Although more recent cases have stressed the importance of notification requirements as safeguards against abuse of surveillance powers,[86] the ECtHR has yet to hold that notification is a *necessary* safeguard in such cases.[87] We note, however, that notification requirements are now a commonplace feature of surveillance laws in a great many jurisdictions including

---

Tariq v Home Office [2011] UKSC 11 at para 128: "The entire point of surveillance is that the person who is subject to it should not be aware of that fact. It is therefore impossible to apply article 6 to any challenge to the decision to place someone under surveillance, at least until notice of termination of the surveillance has been given … It is precisely because the fact of surveillance must remain secret in order to be efficacious that article 6 cannot be engaged. It appears to me, therefore, that the decision in Kennedy ought to have been made on the basis that article 6 was not engaged because the issues that the case raised were simply not justiciable."

[81] See e.g. *Paton v Poole Borough Council* (IPT/09/01/C, 29 July 2010).

[82] See JUSTICE, *Freedom from Suspicion*, at paras 358-364.

[83] Ibid, para 359.

[84] *Klass* at para 57.

[85] Ibid, para 69.

[86] See esp. *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* [2007] ECHR 533 at para 57: "[U]nless criminal proceedings have subsequently been instituted or unless there has been a leak of information, a person is never and under no circumstances apprised of the fact that his or her communications have been monitored. The result of this lack of information is that those concerned are unable to seek any redress in respect of the use of secret surveillance measures against them."

[87] The issue is currently before the Court in the case of *Lüütsepp v Estonia* (46049/13).

Belgium,[88] Bulgaria,[89] Canada,[90] Germany,[91] Ireland,[92] the Netherlands,[93] New Zealand,[94] Sweden[95] and the United States.[96] In his 2013 report to the General Assembly on communications surveillance, moreover, the UN Special Rapporteur on Freedom of Expression stated:[97]

> *Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.*

51. We further note that the Codes of Practice on communications data and encryption keys under RIPA both make provision for notification where a Commissioner establishes that an individual has been "adversely affected" by any "wilful or reckless failure" by a public body.[98] In such cases, the Commissioner is required, "subject to safeguarding national security" to "inform the affected individual of the existence of the Tribunal and its role" as well as to "disclose sufficient information to the affected individual to enable him to effectively engage the Tribunal". It is unclear, however, why these notification requirements should be limited to only cases involving communications data and encryption keys, as well as why the threshold should be restricted to "wilful or reckless" failures. Rather than have the Commissioner make a determination of whether to notify in each case, we consider that the better approach would be to require mandatory notification in each case within a reasonable period (e.g. 6 months following the warrant or authorisation expiring), subject to a judge's decision that notification should be delayed on the basis that that individual's right to an effective remedy is outweighed by some specific investigative need that would otherwise be prejudiced by the disclosure. As with the

---

[88] See Belgian Constitutional Court, *case no. 145/2011*. 22 September 2011 at paras B.82-B92, in which the court held the lack of notification breached the right to privacy under Art 22 of the Belgian Constitution.
[89] See *Lenev v Bulgaria* (41452/07, 4 December 2012) noting that section 34h of the Special Surveillance Means Act 1997 has been amended such that the supervising commission "must inform of its own motion persons who have been unlawfully subjected to secret surveillance, unless notification might jeopardise the purpose of the surveillance, allow the divulgation of operational methods or technical devices, or put the life or health of an undercover agent or his or her relatives or friends in jeopardy" (para 82).
[90] Section 196 of the Criminal Code provides for notification within 90 days of authorisation unless the judge is satisfied that investigations are ongoing or a subsequent investigation would be impeded. Notification cannot be delayed for more than 3 years.
[91] See e.g. *Klass* at para 19 and *Weber and Saravia v Germany* (54934/00, 29 June 2006) at para 136.
[92] Section 10(3) of the Criminal Justice (Surveillance) Act 2009.
[93] Article 34(1) of the Intelligence and Security Services Act 2002 requires notification after 5 years unless certain grounds are met.
[94] Sections 61 and 62 of the Search and Surveillance Act 2012.
[95] Section 11(a) of the 2008 law on Signals Intelligence (SFS 2008:717).
[96] 18 US Code § 2518(8)(d).
[97] UN Special Rapporteur on Free Expression A/HRC/23/40, 17 April 2013, at para 82. See also e.g. the International Principles on the Application of Human Rights to Communications Surveillance, May 2014.
[98] Communications Data Code of Practice at para 8.3. See also the similar provision in the Code of Practice for the Investigation of Protected Electronic Information at para 11.4.

Canadian Criminal Code, however, we recommend that there should be a maximum limit to the period of time for which notification can be delayed, e.g. 5 or 7 years.

52. As regards disclosure and the fairness of the IPT's procedures more generally, we accept that it is appropriate for the Tribunal to respect the agencies' policy of neither confirm nor deny (NCND) in the first instance, and particularly where the subject has not been notified of the surveillance in question. In our view, however, it is important to treat NCND as a starting point only, a defeasible principle that can be set aside where it becomes apparent to the IPT that it is necessary for the complainant to receive disclosure of material in order to effectively present his or her case. As the Vice President of the Court of Appeal held in a recent case, NCND is "not a legal principle" but rather a "departure from procedural norms" that "requires justification" in the same way as public interest immunity.[99] The framework of the IPT's procedures under Part 4 of RIPA, by contrast, do not – in our view – provide the Tribunal with sufficient flexibility to balance national security concerns with those of open justice and natural justice. Among other things, the IPT has no power even to make a declaration of incompatibility, has no formal power to appoint a special advocate to represent the interests of an excluded party, and indeed cannot even notify a party that a closed hearing has been held unless the other party consents. In this way, the framework under Part 4 compares unfavourably with the extensive case law that has developed in relation to closed proceedings in other courts and tribunals since 2001.[100]

53. We also consider that the ouster provision contained in s67(8) RIPA to be incompatible with the requirements of our common law constitution: if an appeal on a point of law is possible from other courts and tribunals employing closed procedures, we can see no good reason why the IPT should be immunised in this manner from the supervision of the higher courts. We therefore recommend that the IPT's procedural rules be significantly relaxed in order to enable much greater disclosure to complainants who have been subject to surveillance in order that they may bring an effective challenge, including sufficient disclosure to enable them to give effective instructions to the special advocate representing them in any proceedings from which they have been excluded.

The Intelligence and Security Committee

54. Although the Intelligence and Security Committee provides important democratic oversight of surveillance powers and the activities of the intelligence services, we note that the accuracy of ISC reports has been the subject of judicial criticism in recent years, first in *R(Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs*[101] and subsequently in the report of Hallett LJ sitting as the Deputy Coroner in the inquest following the 7/7 bombings.[102] Following

[99] *Mohamed Ahmed Mohamed and CF v Secretary of State for the Home Department* [2014] EWCA Civ 559 at para 20 per Maurice Kay VP. See also *DIL and others v Commissioner of Police of the Metropolis* [2014] EWHC 2184 (QB) para 42 per Bean J.

[100] See e.g. *AF v Secretary of State for the Home Department (No 3)* [2010] 2 AC 269; *Bank Mellat v HM Treasury (No 1)* [2013] UKSC 38.

[101] [2010] EWCA Civ 65 at para 168 per Lord Neuberger MR.

[102] Report of Deputy Coroner Hallett LJ under Rule 43 of the Coroner's Rules 1984 (6 May 2011), paras 110-116.

these criticisms, the constitution of the ISC was amended by Part 1 of the Justice and Security Act 2013. We note, however, that although the members of the ISC are now appointed by Parliament rather than the Prime Minister, a person cannot be eligible for appointment unless they have been nominated by the Prime Minister (s1(4)(a) of the 2013 Act). In addition, although the Committee reports now to Parliament instead of to the Prime Minister, it must nonetheless be sent first to the Prime Minister who may require the redaction of any material he considers to be prejudicial to the operation of the intelligence services (s3(4)). In our view, these restrictions are an unnecessary constraint on the Committee's oversight and should be removed.

Retention of communications

55. Notwithstanding that the judgment of the Grand Chamber in *Digital Rights Ireland* invalidating the Data Retention Directive was handed down in April 2014,[103] we note that the government's proposals to address this were not published until July and then enacted on an emergency basis in only three days. It is concerning that legislation on such an important issue was handled in such a manner. It remains unclear, moreover, whether the provisions of ss1-2 DRIPA are compatible with the CJEU's judgment. In our view, much will depend on the regulations and the particular retention notices made by the Secretary of State and we understand that this already the subject of legal challenge. At the very least, we recommend that the power to make retention notices should be removed from the Secretary of State. Instead, retention notices should be issued by a judge on application by the relevant public body seeking retention.

SUMMARY OF RECOMMENDATIONS

56. We recommend as follows:

(i) A single, comprehensive statutory framework should govern the use of intrusive surveillance powers by public bodies. In particular, no public body should have the power to access communications data save by way of this framework.

(ii) Judicial authorisation should be required before any public body intercepts communications, accesses communications data, uses intrusive surveillance (including a covert human intelligence source), issues an encryption notice or a retention notice. The authorising judge should also have the power to direct the appointment of a special advocate to represent the interests of the subjects of surveillance in appropriate cases.

(iii) The existing power to intercept external communications under section 8(4) RIPA should be repealed. At the very least it should be severely curtailed. All warrants and authorisations must be founded on the reasonable suspicion of the authorities that a particular individual has been involved in serious criminal activity.

[103] C-293/12, ECLI:EU:C:2014:238.

(iv) The statutory definition of 'intrusive' surveillance should be tightened to include *any* covert surveillance that either involves or is likely to involve a significant interference with a person's privacy.

(v) The ban on the use of intercept material as evidence in criminal and civil proceedings should be lifted.

(vi) The number of public bodies able to access communications data should be curtailed.

(vii) The oversight functions currently discharged by the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner should be combined into a single statutory oversight body. This body's remit should include oversight of the use of all surveillance powers by public bodies;

(viii) Any person who has been the subject of covert surveillance by a public body should be notified of that fact within a reasonable period following the conclusion of the surveillance, unless a judge is satisfied that that individual's right to an effective remedy is outweighed some specific investigative need that would otherwise be prejudiced by the disclosure;

(ix) The Investigatory Powers Tribunal should be granted the power to appoint special advocates to represent the interests of excluded parties, as well as make a declaration of incompatibility under section 4 of the Human Rights Act. Its procedural rules should also be relaxed to allow much greater disclosure to complainants who have been the subject of surveillance, so that they may bring an effective challenge. This should include sufficient disclosure to enable them to give effective instructions to the special advocate representing them in any proceedings from which they have been excluded. The unsuccessful party should also have a right of appeal to the Court of Appeal on a point of law;

(x) The statutory requirement that candidates for the Intelligence and Security Committee must first be nominated by the Prime Minister in order to be eligible for election should be repealed, as should the power of the Prime Minister to prevent the Committee from publishing material that it considers to be in the public interest to disclose.

APPENDIX: BINGHAM CENTRE EXPERT SEMINAR, 1 OCTOBER 2014

On 1 October 2014, the Bingham Centre for the Rule of Law held an evening conference on the subject of the Investigatory Powers Review led by the Independent Reviewer of Terrorism Legislation, David Anderson QC. Chaired by Eric Metcalfe of Monckton Chambers and the Bingham Centre, the event consisted of three panels: (I) Interception Warrants; (II) Communications Data; and (III) Oversight.

The evening began with an introduction to the Review by David Anderson, and was followed by a discussion of Section 8(1) warrants by Helen Mountfield QC, and Section 8(4) warrants by Matthew Ryder QC, both of Matrix Chambers. Panel II consisted of a discussion of Access to Communications Data under Part 1, Chapter 2 of RIPA by Graham Smith of Bird & Bird, followed by Gillian Phillips, Director of Editorial Legal Services at The Guardian on the subject of RIPA and Professional Privacy. Finally, Panel III concluded with presentations from Tom Hickman of Blackstone Chambers and the Bingham Centre and Eric Metcalfe on the Investigatory Powers Tribunal and the oversight Commissioners and the Intelligence and Security Committee.

The event included lively and and expert debate from the floor and was followed by a reception. The Bingham Centre is grateful to Macfarlanes for hosting the event.

List of Attendees

Name	Organisation
Mr Chris Acton	Macfarlanes
Mr David Anderson QC	Independent Reviewer of Terrorism Legislation
Mr Benjamin Baltzer	Embassy of the Federal Republic of Germany
Mr Martin Bentham	Evening Standard
Dr Jessie Blackbourn	Kingston University
Mr Owen Bowcott	The Guardian
Ms Jennifer Bruce	Ofcom
Mr Tom Bullmore	Treasury Solicitor's Department
Mr Jude Bunting	Doughty Street Chambers
Ms Elinor Buxton	Foreign & Commonwealth Office
Lord Carlile CBE QC	Gray's Inn
Ms Hannah Carter	Ofcom
Mr Rupert Casey	Macfarlanes
Ms Jo Cavan	Interception of Communications Commissioner's Office
Mr Martin Chamberlain QC	Brick Court Chambers
Mr Jan Clements	The Guardian
Mr Martin Coombes	Macfarlanes

Mr Gordon Corera	BBC
Mr Jeremy Courtenay-Stamp	Macfarlanes
Ms Gail Crawford	Lathan & Watkins LLP
Ms Aalia Datoo	Macfarlanes
Dr Andrew Defty	University of Lincoln
Ms Adriana Edmeades	Privacy International
Mr Charlie Edwards	RUSI
Mr Charles Farr OBE	Home Office
Mr Daniel Futter	Metropolitan Police, Directorate of Legal Services
Ms Tessa Gregory	Leigh Day
Mr Stephen Grosz QC (Hon)	Bindmans; Bingham Centre Fellow
Ms Gabrielle Guillemin	ARTICLE 19
Ms Laila Hamzi	Bingham Centre for the Rule of Law
Ms Swee Leng Harris	Bingham Centre for the Rule of Law
Dr Tom Hickman	Blackstone Chambers; Bingham Centre Fellow
Mr Jess Hinings	Ofcom
Ms Sandra Homewood	Bingham Centre for the Rule of Law
Mr Ben Hooper	11 King's Bench Walk
Mr Henry Hughes	187 Fleet Street
Mr Mark Hunting	Ropes & Gray LLP
Mr Ben Jaffey	Blackstone Chambers
Mr Tim Johnston	Brick Court Chambers
Ms Sarah Kavanagh	NUJ
Mr Bernard Keenan	LSE
Mr Eric King	Privacy International
Ms Izza Leghtas	Human Rights Watch
Mr Paul Lomas	Freshfields
Ms Gemma Ludgate	Special Advocates Support Office
Professor Andrew Lynch	University of New South Wales
Mr Daniel Machover	Hickman & Rose
Mr Iain Mackie	Macfarlanes
Ms Jennifer Macleod	Brick Court Chambers
Mr Andy Mather	Macfarlanes
Dr Eric Metcalfe	Monckton Chambers; Bingham Centre Fellow

Ms Helen Mountfield QC	Matrix Chambers
Sir Jon Murphy QPM	Chief Constable, Merseyside Police
Sir David Omand GCB	King's College London
Ms Angela Patrick	JUSTICE
Ms Gillian Phillips	The Guardian
Mr Mark Powell	HM Inspectorate of Constabulary
Ms Charlotte Powell	Furnival Chambers
Dr Tristram Riley-Smith	Centre for Science & Policy, Cambridge University
Mr Matthew Ryder QC	Matrix Chambers
Mr Naz Saleh	Metropolitan Police
Ms Helen Shaw	Inquest
Ms Jessica Simor QC	Matrix Chambers
Mr Graham Smith	Bird & Bird
Ms Justine Stefanelli	Bingham Centre for the Rule of Law
Mr Dominic van der Wal	Special Advocates Support Office
Mr James Welch	Liberty
Ms Harriet Wistrich	Birnberg Peirce & Partners
Mr Julian Wright	Metropolitan Police