Draft Investigatory Powers Bill

Written Evidence to the Joint Committee on the Draft Investigatory Powers Bill

December 2015

For further information contact

Angela Patrick, Director of Human Rights Policy

email: apatrick@justice.org.uk tel: 020 7762 6415

JUSTICE, 59 Carter Lane, London EC4V 5AQ tel: 020 7329 5100

fax: 020 7329 5055 email: admin@justice.org.uk website: www.justice.org.uk

Summary

In 2011, JUSTICE recommended that the Regulation of Investigatory Powers Act 2000 ('RIPA') be repealed and replaced by a modern legal framework for surveillance more suited to a digital age. Reconciling the right to respect for privacy and the security interests of the wider community requires careful consideration, but the public interests in privacy and security are not mutually exclusive. Surveillance is a necessary activity in the fight against serious crime. When targeted, it can play a vital part in our national security.

Building a legal framework for surveillance in the digital age is now a priority. However, JUSTICE is concerned that the Draft Bill, like the Draft Communications Data Bill before it, includes broad provision for untargeted and bulk powers of surveillance. We raise concerns about the compatibility of these powers with the provisions of the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. While others will be better placed to advise the Committee on the practical impact of these powers or the operational case to support them, JUSTICE urges the Joint Committee to subject the Government's legal analysis to close scrutiny before a Bill is presented to Parliament.

JUSTICE focuses on a number of specific issues in our submission:

(i) The Draft Bill should be amended to provide for judicial authorisation of warrants as a default, subject to a limited exception for certification by the Secretary of State in some cases involving defence and foreign policy matters.

(ii) Any provision for judicial authorisation should provide that the Judicial Commissioner is able to conduct a full merits review of the necessity and proportionality of an individual measure.

(iii) The urgent procedure in the Bill should be amended to restrict the capacity for its arbitrary application.

(iv) Any modification of warrants should be made by a Judicial Commissioner.

(v) Judicial Commissioners considering applications should have access to security vetted Special Advocates to help represent the interests of the subject and the wider public interest in protecting privacy.

(vi) The resources for the new Investigatory Powers Commission ('IPC') should not be managed by the Secretary of State (who may be subject to its scrutiny).

(vii) Any drain on the High Court when judges take up appointments as Judicial Commissioners should be offset by the Treasury.

(viii) The independence of the Commission will be paramount to its effectiveness.

(ix) The judicial functions of the Judicial Commissioners and the wider investigatory and audit functions of the Commission should remain operationally distinct. While it would, in our view, be beneficial for the Commissioners to be able to draw upon the wider expertise provided by the staff of the Commission, there should be no doubt about their capacity to take independent decisions on individual warrants.

(x) Judicial Commissioners should be appointed by the Judicial Appointments Commission not the Prime Minister.

(xi) The Draft Bill should be amended to put beyond doubt that the Commission can conduct own-initiative inquiries.

(xii) Clause 171 on reporting of errors should be substantially amended. At a minimum, it should be accompanied by a mandatory disclosure requirement for individuals targeted for surveillance to be provided with information after-the-event.

(xiii) The Draft Bill should be amended to create a safe-route to the IPC, making clear that communications from officials or Communications Service Providers will not be treated as a criminal offence for any purpose.

(xiv) The new right of appeal from decisions of the Investigatory Powers Tribunal is welcome. The Draft Bill should be amended to clarify that a right of appeal lies from all rulings of the Tribunal, not only final determinations. The route of appeal should be clear on the face of the Bill, not left to be determined in secondary legislation by the Secretary of State.

(xv) JUSTICE considers that the Draft Bill should be amended to modernise the procedures of the IPT. This should include an amendment to provide for the IPT to be able to make declarations of incompatibility pursuant to Section 4, Human Rights Act 1998.

(xvi) The Draft Bill should be amended to provide greater protection for legal professional privilege and for the communications of politicians and journalists.

(xvii) The ban on the use of intercepted material in criminal proceedings, in Clause 42, should be removed.

(a) Introduction

1. Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance access to justice, human rights and the rule of law. It is also the British section of the International Commission of Jurists. In 2011, we published *Freedom from Suspicion: Surveillance Reform for a Digital Age,* calling for the wholesale reform of the existing legal framework for surveillance.[1] In anticipation of the publication of the Draft Investigatory Powers Bill for consultation, we published an update to that report, *Freedom from Suspicion: Building a Surveillance Framework for a Digital Age.*[2]

2. We welcome the opportunity to submit written evidence to the Joint Committee on the Draft Investigatory Powers Bill ('the Committee'). We regret the short time available for consideration of the Draft Bill by the Committee and by the wider community. The Draft Investigatory Powers Bill ('the Draft Bill') was published on 4 November and the Joint Committee is required to report by 11 February. In practice, the Joint Committee will conclude its work in around 7 weeks. We are concerned that, to provide scrutiny of a technically and legally complex Bill of almost 300 pages, this timescale is very short and will limit the effectiveness of pre-legislative scrutiny by Parliament, commentators and the wider public.

3. In this submission, JUSTICE focuses principally on issues of authorisation and the judiciary; oversight and the role of the new Investigatory Powers Commission ('IPC') and the Investigatory Powers Tribunal ('IPT'). We raise some wider concerns about the treatment of privileges, legal professional privilege, in particular, and the treatment of intercept material as evidence in legal proceedings. Given the short time available, we focus on the issues most closely allied to our current work and expertise.

4. Where we do not specifically address an issue, or question posed by the Committee, this should not be taken as support for the proposals in the Draft Bill.

---

[1] JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age,* Nov 2011. Hard copies of this report have been provided to members of the Joint Committee. http://www.justice.org.uk/resources.php/305/freedom-from-suspicion Hererin, '*Freedom from Suspicion*'.

[2] JUSTICE, *Freedom from Suspicion: Building a Surveillance Framework for a Digital Age,* Nov 2015. . Hard copies of this report have been provided to members of the Joint Committee. http://2bguk8cdew6192tsu41lay8t.wpengine.netdna-cdn.com/wp-content/uploads/2015/11/JUSTICE-Building-a-Surveillance-Framework-for-a-Digital-Age.pdf Hererin, '*Freedom from Suspicion: Second Report'*.

(b) Background

5. The Draft Bill fulfils a commitment by Government to produce new legislation to replace the Data Retention and Investigatory Powers Act 2014 in draft for consideration by a pre-legislative committee of both Houses. Part 1 provides for a number of offences which relate to the misuse of powers relating to surveillance. Part 2 deals with the interception of communications by security agencies, law enforcement bodies and others. Parts 3 and 4 deal with the retention of communications data and access to that material. These parts replace the Data Retention and Investigatory Powers Act 2014 ('DRIPA'). They expressly empowers the Secretary of State to request the retention of 'Internet Connection Records'. Part 5 governs "Equipment Interference" (also known as hacking or Computer Network Exploitation). Part 6 creates a framework for 'bulk interception' warrants and for bulk warrants for the acquisition of communications data and equipment interference. Part 7 provides for access to bulk personal datasets. Part 8 provides for the creation of a new single oversight body, the Investigatory Powers Commission ('IPC') and proposes a new right of appeal from decisions of the Investigatory Powers Tribunal ('IPT').

6. Since 2011, JUSTICE has recommended that the Regulation of Investigatory Powers Act 2000 ('RIPA') is repealed and replaced by a modern legal framework for surveillance. Reconciling the right to respect for privacy and the security interests of the wider community requires careful consideration, but the public interests in privacy and security are not mutually exclusive. Surveillance is a necessary activity in the fight against serious crime. When targeted, it can play a vital part in our national security.

7. Building a legal framework for surveillance in the digital age is now a priority. In the past year alone, the IPT has found violations of the right to privacy under Article 8 of the European Convention on Human Rights ('ECHR') by the intelligence services on three different occasions, the Divisional Court has disapplied section 1 of DRIPA because it breached the rights to privacy and data protection under the EU Charter of Fundamental Rights,[3] and the Intelligence and Security Committee and the Independent Reviewer of

[3] *Davis, Watson & Ors v Secretary of State for the Home Department and Ors* [2015] EWHC 2092 (Admin). This decision is subject to appeal and the Court of Appeal has referred a number of the questions to the Court of Justice of the European Union. See [2015] EWCA (Civ) 1185.

Terrorism Legislation have each produced major critical reports on the legal framework governing surveillance powers.[4]

8. While the powers sought in the Draft Bill are more readily comprehensible than in the previous, much criticised, Draft Communications Data Bill,[5] many of its provisions provide for the use of untargeted and bulk powers of surveillance:

    a. **Comprehensive and comprehensible?** We welcome the decision in the Draft Bill to move away from the legislative model adopted in the Draft Communications Data Bill, which created broad powers for public bodies and duties for Communications Service Providers ('CSPs') and left details and safeguards to secondary legislation. We welcome the Government's decision to accept the recommendation of the Anderson Review that powers should be avowed in so far as possible. While in practice this approach increases the size of the Bill, we welcome the efforts made by Government to increase clarity in the powers sought.

    The Bill contains 202 clauses and 8 separate Schedules. While lengthy it doesn't replace the Regulation of Investigatory Powers Bill 2000 ("RIPA") in its entirety. The Bill deals with communications surveillance and replaces Parts 1 and 4 of RIPA, together with powers in other pieces of legislation. Other forms of surveillance – including the use of Covert Human Intelligence Sources – will continue to be governed by the outdated provisions in RIPA. Investigators would continue to need both RIPA and the new law to make sense of the UK's surveillance landscape.

    JUSTICE considers that this is a missed opportunity.

    b. Future-proofing? A number of witnesses and Committee members have expressed an interest in exploring whether the Draft Bill is 'future-proof'. In our 2011 report, JUSTICE recommended that any revised surveillance framework

[4] *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (Cm 7948, October 2010), p44 (Herein the 'ISC Review' and *A Question of Trust,* David Anderson QC, June 2015 (Herein *'the Anderson Review'*). In addition, in March 2014 the then deputy prime minister, Nick Clegg MP, asked the Royal United Services Institute to coordinate a panel made up of former members of the police and intelligence services, senior parliamentarians, academics, and business people to investigate the legality, effectiveness and privacy implications of the UK's surveillance programmes. That panel reported its conclusions in July 2015: see *A Democratic Licence to Operate: Report of the Independent Surveillance Review*. Herein '*the RUSI Review*'.

[5] JUSTICE's submission to the Draft Communications Bill Committee can be read here: http://justice.org.uk/draft-communications-data-bill/

should be flexible but robust.[6] However, we recognised that this was an area where 'future-proofing' has been notoriously difficult, not least because of the massive pace of development of new technology and how we use it in our daily lives. At the time when RIPA was passed, no one could have predicted how integrated our lives on and offline would become in such a short period. Indeed, the UK has a long history of legal reform prompted by subsequent determinations that the law has failed to keep pace (from *Malone* to *Liberty v UK*).[7]

It would be regrettable if an ill-placed desire to 'future proof' these measures led to powers which were overbroad and unduly flexible. The Committee may wish instead to consider whether surveillance, by its nature, is an area suited to regular default consideration by Parliament (consider the Armed Forces Act, which must be renewed periodically). The Anderson Review made a number of recommendations to this effect, which the Committee may wish to consider.[8]

c. New powers or old?

The Government is keen to stress its view that many of the powers in the Draft Bill are already authorised by existing legislation, whether in RIPA or other provisions. Although the Home Office and the agencies may consider that powers in the Bill are both lawful and familiar, the legality of many activities is already subject to litigation in the UK and in Europe at the European Court of Human Rights and the Court of Justice of the European Union.[9]

Many of the powers in this Draft Bill are powers being considered by Parliament and the public by the first time. For example:

- *"Thematic warrants"*: Clause 13(2) provides that a Targeted Interception Warrant may apply to a single person, *or* a group of identified individuals, but can have a broader more 'thematic' application. This practice was first avowed in 2015, during the ISC Review, which discovered that the reference to a specified "person" for a targeted interception warrant under section 8(1) RIPA had been read to include, by virtue of section 81, "any

[6] *Freedom from Suspicion,* para 147. Importantly, flexibility cannot be sought at the cost of legal certainty. Overly broad powers or discretions are likely to render surveillance powers incompatible with Article 8 ECHR.
[7] *Malone v UK*, App No 8691/79, 2 August 1984, *Liberty v UK*, App No 58243/00, 1 October 2008. See *Freedom from Suspicion,* paras 59 – 61.
[8] Anderson Review, para 12.96 – 12.97.
[9] Cases currently being pursued are summarised by the Anderson Review in Chapter 5. They include *Big Brother Watch and Ors v UK*, App No 5810/73 and *Ten Human Rights Organisations v UK* (*Liberty & Ors*).

organisation and any association or combination of persons". Internal guidance on this point had never been published before the ISC Review.

In practice, this is a substantial expansion of the targeted interception warrant as debated by Parliament during the passage of RIPA. In effect, the language in Clause 13 could provide for the interception of the communications of a large category of persons, loosely defined.

- *Bulk Equipment Interference*: Clause 135 deals with warrants for bulk equipment interference. The Equipment Interference factsheet suggests that this power is not new, referencing Section 5 and 7 of the Intelligence Services Act 1994 and section 93 of the Police Act 1997 and that the practice of wide-spread use of equipment interference by the agencies and police was avowed in February 2015.

  The use of this power in bulk has not yet been avowed and the conduct of bulk hacking activities remains subject to litigation.[10]

- *Data Retention and Investigatory Powers Act ('DRIPA') and communications data retention*: DRIPA was passed on an emergency timetable with extremely limited time for Parliamentary scrutiny.[11] Its measures are subject to a sunset clause which will see it lapse at the end of 2016. The provisions in Parts 3 and 4 although broadly based on DRIPA, include new features, including provision for the retention of Internet Connection Records and for the creation of "filtering" arrangements. These reflect features of the controversial Draft Communications Data Bill, previously considered and criticised by an earlier Joint Committee.

  This Bill provides a key opportunity in Parliament for detailed debate on the legal framework for the retention and processing of communications data. The foundation of these powers in DRIPA should not provide a reason to curtail full scrutiny of the justification for the powers proposed in the Draft Bill.

[10] In ongoing litigation involving Privacy International, documents which post-date the Draft Bill express doubt on whether bulk powers are avowed or are sought anew. See: https://privacyinternational.org/sites/default/files/Schedule_Of_Public_Statements_CNE_Final.pdf

[11] Consideration of the Bill was conducted over a seven day period late in the Parliamentary term.

(c) Privacy and surveillance

9. That each of the distinct acts of collection, retention and use of personal information is engaged by our right to respect for private life, home and correspondence is trite law.[12] The protection of private correspondence is guaranteed by international and European law, including in both Article 8 of the European Convention on Human Rights and the equivalent provision of the European Charter of Fundamental Rights.[13]

10. In many instances, an individual subject to surveillance may never know whether his information has been reviewed or what has been retained. Only in the limited circumstances when the information obtained is used in a trial or when an authority acknowledges the surveillance may an individual be able to challenge its propriety. Accordingly, in these circumstances, there is a significant obligation on the State to ensure that surveillance powers are closely drawn, safeguards appropriate and provision made for effective oversight: "*[it is] unacceptable that the assurance of the enjoyment of a right … could be…removed by the simple fact that the person concerned is kept unaware of its violation."*[14]

11. The European Court of Human Rights has stressed that the justification of any surveillance measures places a significant burden on States to adopt the least intrusive measures possible: "*[P]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.*"[15]

---

[12] In *Malone v UK* (1984) 7 EHRR 14, the Court considered the attachment of a 'meter check printer' to a telephone line for the purposes of recording the time calls were made, to whom and for how long. The Court considered that the collection of this information engaged the right to privacy, but in these circumstances could be justified by reference to the commercial need for a supplier of services to legitimately ensure a subscriber is charged correctly. This use was proportionate and justifiable. However, passing the information to the police without statutory authority and relevant safeguards against abuse was not. See, for example, paras 56 – 84. It is worth noting the gathering and collation of the information here is justified by the commercial need to retain information. The Draft Bill does not limit its effect to material already held by suppliers and operators, but will require the generation or retention of data not needed for any commercial purpose. The question of justification here goes to whether the generation or retention of this information can be justified for the purposes set out by the Home Office in connection with the potential for some communications to inform investigations and inquiries by public authorities. In *Amann v Switzerland* (2000) 30 EHRR 843, for example, the Court held that the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted. In *Rotaru v Romania* (2000) 8 BHRC 449, at para 43, the Court stressed that even 'public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities'.

[13] Article 7 CFREU. See also the International Covenant on Civil and Political Rights, Article 17.

[14] (1978) 7 2 EHRR 214, paras 36, 41.

[15] Ibid, para 42. See also Para 49: *'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 means they deem appropriate'.*

12. While safeguards are crucial to the legality of surveillance powers, they are not conclusive, nor determinative. Although the Draft Bill provides for safeguards designed to ensure that powers are applied proportionately, it is for Parliament to be satisfied that the powers *themselves* are necessary and proportionate.

13. Others are better placed than JUSTICE to provide detailed evidence on the operational case for reform and the proportionality of the powers proposed. However, we are concerned that the expansion of untargeted and bulk powers of surveillance is at odds with existing legal practice.

14. The further powers move away from traditional forms of surveillance, targeting a named individual, on the basis of reasonable suspicion that they are involved in serious criminal offending, the greater the risk to personal privacy and the broader the potential for arbitrary application and abuse. This is particularly significant in circumstances where individuals may be unable to access the mainstream justice system to challenge unlawful behaviour by public authorities or to seek redress for the violation of their individual rights.

15. Importantly, the UN Special Rapporteur on Human Rights and Counter-Terrorism had expressed concern over the breadth and impact of this kind of untargeted power: "*the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether*".[16]

16. There is limited legal authority from the European Court of Human Rights to support the lawful use of such untargeted or bulk surveillance powers:

    a. Most recently, in *Zakharov,* the Court subjected a Russian law on the bulk interception of mobile phone communications to close scrutiny and found it incompatible with the right to privacy. Although provision was made in that case for judicial authorisation for access to any such material, the untargeted power was held to be incompatible with Article 8 ECHR. The measure was overbroad and subject to abuse.[17]
    b. In *Digital Rights Ireland,* the Court of Justice of the European Union considered the mass retention of citizens' communications data. Testing the Data Retention

[16] A/69/397, paras 12.14.
[17] *Zakharov v Russia,* App No 47143/06, 4 December 2015.

Directive against a framework of safeguards, the measure was found disproportionate as it failed to make provision for specific safeguards, including, that "above all", access by national authorities was not made dependent on *"prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary."*[18]

c. In *Schrems,* the Court of Justice of the European Union stressed that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life*".[19]

d. In *Liberty v UK,* the Court emphasised: "*The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance on the other*".[20]

17. Beyond Europe, we note that a number of countries have recently changed their laws to restrict the ability of agencies and authorities to access communications data in bulk, including the United States, indicating that the benefit gained by such activities was minimal and disproportionate in light of the intrusion on innocent citizens lives.[21]

18. The untargeted and bulk powers in the Draft Bill must be subject to particularly close scrutiny by Parliament and an operational case for each subject to debate and test by the Committee.[22]

19. We consider below some of the new safeguards proposed in the Draft Bill.

(d) Authorising surveillance

20. The Human Rights Memorandum accompanying the Draft Bill explains the Government's view that it's primary safeguard is "the introduction of an authorisation process which includes prior approval of warrants by independent judges called Judicial

[18] *Digital Rights Ireland,* C-293/12 and C-594/12
[19] C-362/14, 6 October 2015.
[20] *Liberty v UK,* para 63.
[21] Earlier this year, bulk powers to retain telephone data in the US were allowed to lapse (Section 215, Patriot Act). This followed extensive criticism by the Privacy and Civil Liberties Oversight Board, which concluded that the material had not had a significant benefit for investigations. A number of US based intelligence professionals have expressed similar scepticism. One, William Binney, has already provided written evidence to the Committee. A similar experience occurred in Denmark, where similar bulk retention powers were judged ineffective and repealed.
[22] An operational case has been provided in the materials supporting the Draft Bill, but this only addresses the powers which relate to Internet Connection Records.

Commissioners". Termed a "double-lock", JUSTICE is concerned that the Government's description of this safeguard is misleading. The provisions in the Draft Bill fall far short of the mechanisms for prior judicial authorisation or judicial warrantry applied in other countries.

21. JUSTICE is particularly concerned that the Draft Bill: (i) conflates authorisation and review; (ii) is inconsistent in its approach to judicial involvement, (iii) provides insufficiently specific triggers for warranting powers throughout the Bill, and in particular, in connection with new thematic or bulk, untargeted powers; (iv) provides for an inappropriately broad mechanism for urgent authorisation of warrants; (v) permits the modification of warrants without sufficient oversight; and (vi) makes limited provision for to ensure that the procedure for authorisation is fair and takes into account the interests of the individual subject to surveillance and the wider community in the protection of privacy.

(i) Judicial authorisation or review?

22. The Draft Bill provides that the primary decision maker for some surveillance decisions will be the Secretary of State or a senior official, whose decision will then be subject to review by a Judicial Commissioner. The Judicial Commissioner will review whether a warrant is (a) "necessary on relevant grounds" and (b) "whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved". In conducting a review, the Commissioner must "apply the same principles as would be applied by the court on an application for judicial review."[23] See, for example, Clause 19 (Targeted Interception, Examination and Mutual Assistance).

23. The Anderson Review recommended that all interception warrants (and bulk warrants) should be judicially authorised, concluding that "*the appropriate persons to perform this function would be senior serving or retired judges in their capacity as Judicial Commissioners.*"[24]

24. A two stage "certification" model was recommended in cases involving "defence of the UK and foreign policy". In these cases alone the Secretary of State should have the power to certify that the warrant is required in the interests of the defence and/or the foreign policy of the UK. The judge should have the power to depart from that certificate,

[23] Clause 19. However, these provisions are repeated in other clauses of the Bill.
[24] Anderson Review, para 14.47 at seq.

the Independent Reviewer suggests, "*only on the basis of the principles applicable in judicial review*" which he notes would be "*an extremely high test in practice, given the proper reticence of the judiciary where matters of foreign policy are concerned*".[25] The judge would remain responsible for verifying whether the warrant satisfied the requirements of proportionality and other matters falling outside the scope of the certificate.

25. Unfortunately, throughout, the Draft Bill adopts a two stage process, which provides for executive or administrative authorisation, subject to judicial review. In evidence, the Government has explained its view that it is appropriate for the purposes of accountability to Parliament that the Secretary of State remain involved.

26. In 2011, we concluded that it was this "*very accountability that leads at least some of them to disregard the rights of unpopular minorities in favour of what they see as the broader public interest. The same mandate that gives elected officials their democratic legitimacy is what makes them so ill-placed to dispassionately assess the merits of intercepting someone's communications*".[26] In practical terms, however, we note that there is, in any event, little prospect of government ministers being held to account for the interception warrants they sign so long as the details of those warrants remain secret. Among other things, Section 19 of RIPA makes it a criminal offence to disclose the existence of an interception warrant unless authorised to do so. If accountability is to be an effective safeguard, it must be more than nominal. Genuine accountability, however, would require a degree of transparency that would be impossible to square with the need for operational secrecy. If it is right, therefore, that details of interception decisions must be kept secret in order to remain effective, it would better for that authorisation to be made by someone who is already institutionally independent rather someone who is only nominally accountable.

27. A two stage model might be appropriately applied in cases involving the assessment of defence decisions and foreign policy, principally targeting communications outside of the UK. However, JUSTICE supports the original recommendation of the Anderson Review that judicial warranting should be the default mechanism for the authorisation of most surveillance decisions in the UK. The Draft Bill should be amended to provide for a single stage process of prior judicial authorisation as a default, with exception provided for a limited class subject to the certification of the Secretary of State.

[25] Ibid, para 14.64.
[26] *Freedom from Suspicion*, para 85.

28. In any event, the Draft Bill should be amended to put beyond doubt that the Judicial Commissioners must routinely conduct a full merits based assessment of necessity and proportionality:

    a. The principles of judicial review, while long-standing, are not fixed in stone, they can be altered by later judicial practice or statutory intervention (see, for example the Criminal Justice and Courts Act 2015).
    b. Since the introduction of the Human Rights Act 1998, it has been trite law that the reviewing role of any judge assessing necessity and proportionality in human rights cases *must* involve a substantive assessment.[27]
    c. However, the standard of review, even in ordinary judicial review claims, is a flexible one. In some circumstances, a reviewing court will be required to conduct 'anxious scrutiny' (for example, in cases involving breaches of fundamental rights in the common law). In other cases, the court will be expected to afford the relevant decision maker a very wide margin of discretion.[28]
    d. In a recent article, Lord Pannick QC has expressed his view that "The Home Secretary's proposals for judicial involvement *in national security cases* adopt, I think, the right balance in this difficult area" (emphasis added).[29] We agree with Lord Pannick QC and the Anderson Review, as we explain above, that in *some key national security* cases the "review model" might strike an appropriate balance.
    e. There is no guarantee that the close scrutiny applied in the cases cited by Lord Pannick QC will necessarily be applied to applications pursuant to the process in the Draft Bill. While this kind of anxious review has been consistently applied by the courts in cases involving threats to life or limitations on liberty, it is far from certain that this approach would apply consistently to applications following the procedure in the Draft Bill.[30]

[27] *Miss Behavin' Ltd* [2007] 1 WLR 1420
[28] See, for example, *Rehman v Secretary of State for the Home Department* [2001] UKHL 47
[29] *Safeguards provide a fair balance on surveillance powers,* The Times, 12 November 2015. Lord Pannick references the involvement of courts in other decisions engaging national security. JUSTICE notes that the treatment of cases under the Terrorism Preventions and Investigation Measures Act 2012 and by the Special Immigration Appeals Commission, are not directly comparable to the ex parte application for a warrant envisaged in the Draft Bill. In those cases, albeit subject to an exceptional closed material procedure, the subject of the relevant order is aware of the proposed interference with his or her rights and can make submissions to rebut the Secretary of State's position.
[30] Consider, for example, *Home Office v Tariq* [2011] UKSC 35, [27]. The applicant sought the same guarantees applicable in TPIMs procedures – the provision of a gist of material considered in closed material proceedings. The Court distinguished this case from TPIMs determinations, which involve liberty of the individual, and similarly noted that a high standard was not expected in other significantly serious cases outside the scope of liberty claims: "Mr Tariq also has an important interest in not being discriminated against which is entitled to appropriate protection; and this is so although success in establishing discrimination would be measured in damages, rather than by way of restoration of his security clearance (now definitively withdrawn) or of his position as an immigration officer. But the balancing exercise called for in para 217 of the European Court's judgment in A v United Kingdom depends on the nature and weight of the circumstances on each side, and cases

f. Importantly, in an ordinary judicial review claim or a statutory appeal, a claimant will be able to challenge the standard of review applied in practice by a judge. Surveillance applications will necessarily be *ex-parte*. Following the procedure in the Bill, there will be no opportunity for external scrutiny of the standard applied other than in the post-hoc review by the IPC or if the Secretary of State chooses to challenge the approach of the Judicial Commissioner and request a fresh decision by the Investigatory Powers Commissioner. (In the latter case, of course, it will be open to the Secretary of State to argue that the standard of review has been *too* robust.)

g. In any event, even if close scrutiny is applied in some *national security* cases, it is unlikely that this safeguard would be sufficiently robust in others, including in the significant proportion of applications relating to law enforcement and the prevention and detection of crime.

29. We encourage the Committee to examine whether it is appropriate for Ministers to be involved at all in applications arising in the course of law enforcement operations. The Draft Bill should be amended to provide for a single step authorisation process in most circumstances, except in respect of applications involving the interference with communications of and between individuals outside the UK, engaging defence and foreign policy matters. In these circumstances, any request may be certified by the Secretary of State, subject to review by the Judicial Commissioners. However, in ordinary applications in the course of any criminal investigation, including domestic counter-terrorism activities, warrants should be subject to prior judicial authorisation alone.

(ii) Consistency and Communications Data

30. In any event, only some surveillance decisions in the Draft Bill benefit from any judicial involvement. There are some exemptions from review which create particular inconsistencies which the Committee might wish to consider. In others, there are differences of approach which may be difficult to justify. For example, the Secretary of State will be able to modify the terms of warrants for equipment interference by the security services without judicial approval, whereas modifications to police warrants must

---

where the state is seeking to impose on the individual actual or virtual imprisonment are in a different category to the present, where an individual is seeking to pursue a civil claim for discrimination against the state which is seeking to defend itself." (JUSTICE is intervening in the case of *Tariq v UK,* currently being considered by the European Court of Human Rights).

be reviewed by a judge.[31] There are a number of particular carve-outs for national security cases which the Committee may wish to consider. The acquisition of communications data, for the purposes of national security, does not appear, for example, to require supervision by a person independent of the application (See Clause 47(2) – (3)). Similarly constraints designed to provide limited additional protection to journalistic sources when communications data is sought will not apply to the security agencies (Clause 61).

31. All decisions on retention of communications data are taken by the Secretary of State, without provision for review (Clause 71). Access to communications data, will generally be by someone within the same organisation as the person seeking permission or by the Secretary of State (See Clause 46). A judge will only be involved in cases involving local authorities and in circumstances involving journalistic material.

32. JUSTICE considers that there is a strong case that by failing to subject retention and access to communications data to judicial oversight, the legal framework in the Draft Bill may be out of step with international standards:

    a. The Court of Justice of the European Union ('CJEU') in the *Digital Rights Ireland* decision placed a particular premium on oversight by a judicial or other independent administrative body (see above).
    b. The Government's Human Rights Memorandum appears to suggest that this decision is broadly irrelevant to the scope of domestic legislation. JUSTICE considers that this view is surprising (although we understand that the Court of Appeal has recently asked the CJEU to further elaborate on the scope of this case).[32] Not least, the analysis of the Court in respect of the kinds of safeguards necessary for the Directive, which applied across the Union, is likely to be relevant to the safeguards considered suitable for national measures. That analysis is likely to inform the consideration by national courts of necessary safeguards (see consideration by the High Court and Court of Appeal in *Davis & Watson)*[33] and by other international forums, including at the European Court of Human Rights.

[31] Clause 96.
[32] See Human Rights Memorandum, para 100. See *R (David) v Secretary of State for the Home Department* [2015] EWCA (Civ) 1185.
[33] See *Davis, Watson & Ors v Secretary of State for the Home Department and Ors* [2015] EWHC 2092 (Admin). This decision is subject to appeal and the Court of Appeal has referred a number of the questions to the Court of Justice of the European Union. See [2015] EWCA (Civ) 1185.

c. Although there is limited guidance on retention from Strasbourg, the less targeted a compulsory power exercised, the greater the likelihood the provision will be considered disproportionate. The Court has generally been hostile to the application of blanket rules applied to personal information, particularly in the criminal justice system. In *S & Marper,* for example, the Court robustly rejected domestic law on the retention of DNA and fingerprints taken from innocent adults and children. Although retention of the material served a legitimate aim – the prevention and detection of crime – its blanket application was disproportionate, particularly in light of the impact on innocent individuals and the stigma of association with a criminal database.[34] Most recently, in *Zakharov,* the European Court of Human Rights again emphasised that surveillance powers must crucially be targeted at the prevention and detection of serious crime or the protection of national security: *"Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security*".[35]

33. While the legality of bulk surveillance models is currently being tested at both the CJEU and in Strasbourg, the existing case law supports an assessment that the *less* targeted the measures the *more* likely that robust authorisation and oversight measures will be necessary.

(iii) Specificity, targeting and warrants

34. The breadth of the triggers which may justify the use of the powers in the Bill and the scope of the application of individual warrants or powers require close scrutiny. In particular, the gateway to a number of thematic or bulk powers may be insufficiently precise to be compatible with Article 8 ECHR.

35. In any event, the breadth of application of some of the powers concerned may make it particularly difficult to assess necessity and proportionality in any meaningful way,

[34] *S & Marper v UK,* App No 30562/04, 4 December 2008.
[35] *Zakharov*, para 260.

undermining the ability of any authorising body, including a Judicial Commissioner to act as a significant safeguard against abuse.

36. The main grounds in the Draft Bill for issuing surveillance warrants are (a) "in the interests of national security", (b) "for the purposes of preventing or detecting serious crime" and (c) "in the interests of the economic well-being of the UK, in so far as those interests are also relevant to the interests of national security". Communications data can be accessed by a larger number of authorities and for a greater variety of purposes (including public health, public safety and for the collection of taxes, duties or levies, for example).

37. While the Strasbourg court has been keen to stress that the grounds for surveillance need not be defined in absolute terms, a sufficient degree of certainty is necessary in order to allow an individual to understand when they might be likely to be subject to surveillance.

38. The Court in *Zakharov* expressed particular concern about a Russian surveillance law which permitted bulk collection of mobile telephone data for reasons connected with "national, military, economic or ecological security", noting that "*which events or activities may be considered as endangering such types of security interests is nowhere defined in Russian law*".[36] The only safeguard against abuse of this absolute discretion was effective judicial authorisation, capable of conducting a more focused assessment of the proportionality of an individual measure. However, the authorisation process in that case proved inadequate:

> *"Turning now to the authorisation's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security".*[37]

39. The Court went on to conclude that the quality of review by the Russian courts was inadequate to specify the risk posed by any particular individual or the necessity and proportionality of subjecting them to surveillance, noting:

[36] *Zakharov,* para 246.
[37] *Zakharov,* para 260.

"courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed"

"the failure to disclose the relevant information to courts deprives them of the power to assess whether there is a sufficient factual basis to suspect the person in respect of whom operational-search measures are requested of a criminal offence or of activities endangering national, military, economic or ecological security".[38]

40. JUSTICE is concerned that a similar degree of scrutiny is likely to be impossible, or at least exceptionally difficult, when applied in the context of the thematic or bulk powers in the Draft Bill, which may apply to ill-defined categories or groups of people (or to the communications of most individuals in the UK, provided they are using particular services based outside the United Kingdom, like Facebook or GMail).[39] For example, the Draft Equipment Interference Code of Practice, explains that individuals who are "not intelligence targets in their own right" may be the subject of warrants for thematic equipment interference.[40]

41. In these circumstances, the ability of a judicial authorisation procedure to reliably test necessity and proportionality of the impact of a measure on an individual is likely to be inherently limited, and as such, is unlikely to operate as a significant safeguard against abuse.

(iv) Urgency

42. Throughout the Draft Bill judicial review is accompanied by an alternative 'urgent' procedure (see for example, Clause 20). The scope of the urgent mechanism is extremely broad and ill-defined, and in our view could fatally undermine any safeguard provided by any mechanism for judicial authorisation or review.

43. The Bill provides that a urgent warrant by be issued by the Secretary of State in any case which she "considers" there is "an urgent need". Urgent need is not defined. An urgent warrant must be subject to judicial review within 5 days. If a judge is satisfied that the surveillance should never have been authorised, they may (but are not required to) order that the material gathered is destroyed.

[38] *Zakharov,* paras 265 and 261.
[39] The Anderson Review notes that the consideration of the existing RIPA model in *Kennedy v UK* considered targeted surveillance, not bulk measures of the kind contemplated in the Draft Bill. See para 5.43.
[40] Draft Code of Practice on Equipment Interference, February 2014, Home Office.

44. JUSTICE considers that this provision is unnecessary and would permit the already limited judicial scrutiny proposed in the Draft Bill to be side-stepped in ill-defined circumstances and for unspecified purposes.

45. JUSTICE recognises that surveillance decisions may be required urgently. However, urgent decision-making would be familiar to any judge or former judge appointed as a Judicial Commissioner. From search warrants pursuant to the Police and Criminal Evidence Act 1984 to High Court duty judges dealing with injunctions and deportation, urgent orders in family cases for child protection, considering evidence and taking decisions on short notice at anti-social hours forms a familiar part of the judicial experience. There are a number of provisions for warrantry in connection with the investigation of serious crime (including terrorist offences), and no concern has been raised about the inability to raise a judge an appropriate hour to allow an investigation to continue without undue delay.[41] There are likely to be multiple Judicial Commissioners capable of serving on a duty rota. In practice, urgent decision making is likely to be less of a burden for the cadre of Commissioners than for a single Secretary of State.[42]

46. Very recent guidance from the Grand Chamber of the European Court of Human Rights affirms that this kind of urgent model is likely to be inadequate to protect the privacy rights of individuals subject to surveillance. In *Zakharov,* the Court considered an urgent authorisation mechanism in operation in Russia, which provided for administrative authorisation, with independent review within 48 hours. Even in these limited circumstances, the Court was extremely critical of the use of broad and ill-defined discretions to trigger an emergency procedure: "*The domestic law does not limit the use of the urgency procedure to cases involving an immediate serious danger to national, military, economic or ecological security. It leaves the authorities an unlimited degree of discretion in determining in which situations it is justified to use the non-urgent judicial procedure, thereby creating possibilities for abusive recourse to it*".

47. While the proposals in this Draft Bill provide for subsequent review within five days there is no clear requirement for material to be destroyed, even if the material is gathered unlawfully, or for steps to be taken to provide redress for the unlawful surveillance conducted. Instead those matters remain within the discretion of the individual Judicial Commissioner, who must hear arguments from the Secretary of State, subject to appeal

[41] For example, Section 40, Terrorism Act 2000 requires a search warrant to be issued before premises can be searched in connection with terrorist offences in the Act

[42] The Committee has already heard evidence about the strain placed on Ministers by the warranting process. This burden was key in the Independent Reviewers conclusion that judicial warrantry was necessary in the new legislative framework. See *Anderson Review*, para 14.54.

to the Investigatory Powers Commissioner. We are concerned that this model creates little disincentive against abuse of the urgent procedure.[43]

(v) Modification

48. JUSTICE is concerned about the breadth of provision in the Bill for warrants to be modified after the authorisation process is complete. These provisions are not consistent in their application throughout the Draft Bill and it is far from clear why the Government considers such broad provision for self-authorised modification might be appropriate.[44] Clause 26, for example, provides that Targeted Interception, Targeted Examination and Mutual Assistance Warrants, including those thematic warrants targeting groups of persons or places, could be modified by the Secretary of State or a senior official at any time, to add or remove any person, place or organisation. It would also permit a minor modification by the person to whom the warrant is addressed, or their colleagues, to vary such names or descriptions or to add, vary or remove any other "factor" specified in a warrant. These modifications can be made without any further judicial authorisation.[45] JUSTICE is particularly concerned that this broad power could entirely side-step the limited judicial oversight provided in this part of the Bill.

49. The breadth of such modification provisions are of particular concern in the context of "thematic interception warrants" or any bulk warrant in the Draft Bill. For example, clause 13 makes clear that Targeted Interception Warrants may cover not only identified individuals or premises, but may also cover groups of persons sharing a common purpose or activity as well as or more than one set of premises or organisations, where these are part of the same investigation. The legality of this kind of untargeted surveillance remains untested, and has only recently been avowed (during the course of the ISC inquiry). If the modification power in Clause 26 applies to thematic interception; as it appears it must, this could, for example, mean a warrant for interception of the

[43] See *Zakharov*, [266] and *Association for European Integration and Human Rights and Ekimhzhiev* App No 62540/00, 28 June 2007, [16]. By contrast in this latter case, the Court considered a Bulgarian law, which allowed for an urgent warrant subject to review and authorisation by an independent judge within 24 hours. The power was only available in circumstances where there was an "immediate risk that a serious intentional offence would be committed" or "an immediate threat to national security". In this case, the reviewing judge had the discretion to decide whether material obtained should be retained or destroyed. Yet, the Court only accepted this procedure on credible evidence that the use of this power was intended to be "used sparingly and only in duly justified cases" (para [82]). The relevant law was found incompatible with the right to respect for private life for other reasons (it failed to provide for subsequent oversight, notification after-the-event, and adequate provision for access to redress).

[44] For example, in connection with the provision in the bill for equipment interference – hacking – different authorisation models apply to hacks by the security agencies or the police. The agencies are authorised by warrant from the Secretary of State, subject to judicial review, police hacks are self-authorised within the force, subject to judicial review. Modifications minor and major – including to names, places and conditions – can be made by the Secretary of State without review. Modifications to police warrants must be subject to judicial review. See Clause 96.

[45] By way of contrast, Clause 96, which deals with the modification of warrants for equipment interference, provides that any modification which would have been subject to judicial approval on application cannot take effect without judicial authorisation. See Clause 96(6).

communications of a group of students at the University of London could, in principle, be legitimately expanded to cover all students in the UK without further judicial approval.

50. In *Zakharov,* the Grand Chamber not only confirmed the importance of independent judicial authorisation, it made clear that part of the value of the safeguard lay in ensuring legal certainty about the scope of warrantry.[46]

51. JUSTICE considers that *any* substantive change to a warrant should be subject to fresh judicial approval. The Draft Bill should be amended accordingly.

(vi) Procedural matters

52. Firstly, the Draft Bill should be amended to make clear that a security-vetted Special Advocate should be appointed to represent the interests of the subject and the wider public interest as necessary. For the past 15 years, it has been a statutory requirement in Queensland to appoint a Public Interest Monitor to supervise all applications for the use of surveillance devices.[47] In October 2011, Victoria also introduced a Public Interest Monitor in respect of applications for interception and surveillance.[48] In March 2015, the Australian federal government announced that it would introduce a Public Interest Monitor in relation to applications for access to journalists' communications data.[49]

53. Secondly, it should be open to the Judicial Commissioners to issue clear guidance on the law and its application. This could be achieved, for example, by permitting Judicial Commissioners to produce reasoned decisions on a point of law or principle, in any particular application, subject to anonymisation and redaction as necessary to protect sensitive material damaging to national security. The recent experience of the IPT in publishing judgments on law and principle might inform this process.

54. Finally, if the Draft Bill retains the two-stage 'review' model, it should be made explicit that all the material provided to the Secretary of State on application for the relevant warrant (together with any relevant updating material) must also be provided to the Judicial Commissioner.

---

[46] See [264] – [265]: "As regards the content of the interception authorisation, it must clearly identify a specific person to be placed under surveillance or a single set of premises…". Notably, the Anderson Review would have required all substantive changes to warrants to be subject to judicial authorisation. See Recommendations 34, 39 and 49. This would have included, particularly, any change to names or premises.

[47] See Police Powers and Responsibility Act 2000 (Qld) s 740(1) and Crime and Misconduct Act 2001 (Qld) s324(1).

[48] Public Interest Monitor Act 2011 (Vic).

[49] See e.g. "Abbott government and Labor reach deal on metadata retention laws", Sydney Morning Herald, 19 March 2015.

55. While the Government has again compared Communications Data – including the collection of new ICR data – to a telephone bill, the reality is that this material is far more intrusive. In its unanimous decision in the 2014 case of *Riley v California*, for instance, the US Supreme Court noted that mobile phones "*place vast quantities of personal information literally in the hands of individuals*".[50] Indeed, Chief Justice Roberts remarked that: "*it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives— from the mundane to the intimate*".[51] That record includes not just the *content* of communications but also, the Court held, the data relating to those communications, e.g. a person's search history and location data.[52] The Court went on to approve Justice Sotomayor's 2012 description of GPS data as producing "*a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations*".[53]

56. Officials, agencies and others have expressed concern about the administrative burden that judicial oversight of communications data retention and requests for access would create. However, different models might be considered to accommodate the bulk of requests for communications data. In *Freedom from Suspicion,* we recommended that certain types of data (including basic subscription data) might be exempt from prior judicial authorisation when sought by law enforcement agencies or the emergency services.**[54]** The Anderson Review would have subjected 'novel or contentious' access requests to judicial oversight.**[55]** An alternative means to reduce the administrative burden could be to subject requests for communications data to judicial oversight by

[50] 573 US (2014) per Roberts CJ at 9.

[51] Ibid, 19. The Chief Justice also noted that the very term "*cell phone*" was itself "*misleading shorthand*" since "*many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers"* (ibid, 17). Before mobile phones "*a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy*" simply because *"[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read*", whereas "*the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones*" (ibid, 17-18).

[52] For example, "*[a]n Internet search and browsing history … can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building*".

[53] 565 US (2012) at 3, cited at *Riley*, ibid, at 20.

[54] *Freedom from Suspicion*, para 182-186.

[55] Both the ISC and RUSI reports acknowledged the sensitivity of communications data. For its part, the ISC sought to distinguish "basic" data used to identify the "who, when and where" of a communication from what it described as "communications data plus", which would encompass "details of web domains visited or the locational tracking information in a smartphone". It suggested that, whereas basic data did not require the same protection as the content of communications, there were nonetheless "legitimate concerns" that "communications data plus" had "the potential to reveal details about a person's private life (i.e. their habits, preferences and lifestyle) that are more intrusive" and therefore required greater safeguards (though it did not spell out what those safeguards should be).

specially trained magistrates, operating as part of the IPC. We consider this recommendation in some detail in *Freedom from Suspicion: Second Report.*[56]

(e) The Investigatory Powers Commission

57. One of the key recommendations of *Freedom from Suspicion,* in 2011, was the need to both strengthen and streamline the existing oversight arrangements for the use of surveillance powers by public bodies. In the first instance, we recommended that increasing the use of prior judicial authorisation would significantly reduce the need for ex-post facto oversight as well as the burden on the IPT.

58. More generally, however, we observed that the oversight arrangements under RIPA were unnecessarily complex and ineffective: in the case of encryption notices under Part 3, for instance, responsibility for oversight is spread across three different commissioners: the Intelligence Services Commissioner (where the notice is sought by the intelligence services), the Chief Surveillance Commissioner (where the notice is sought by the police) and the Interception of Communications Commissioner (if the notice relates to intercepted communications). We recommended, therefore, that the oversight functions of the Interception of Communications Commissioner and the Intelligence Services Commissioner should be transferred to the Office of the Chief Surveillance Commissioner, with that body assuming sole responsibility for the oversight of surveillance powers by the police, intelligence services and other law enforcement bodies.

59. Against this background, we welcome the provision in the Draft Bill to consolidate the responsibilities of the diverse commissioners in a single Investigatory Powers Commission ('IPC'). However, whether that body succeeds in becoming a robust, transparent and accountable public facing body, which increases public confidence, will depend very much on its structure, powers and resources. We are concerned that provisions in the Draft Bill may inhibit the independence of the IPC or limit its effectiveness in practice. We address a number of concerns, below.

[56] *Freedom from Suspcion: Second Report,* para 27.

(i) Resources

60. The effectiveness of the IPC and the confidence of the public will hinge not only on the independence of the body and the powers granted by Parliament, but on the resources available to it. We share the concern expressed by Sir Stanley Burnton that the budget holder for the Commission will be the Secretary of State whose conduct – or the conduct of agencies or bodies for which she is responsible - will be subject to its scrutiny.[57] Even in circumstances where a more diffuse overlap between the conduct of an auditing body and its sponsoring department exists, Parliament has previously expressed concern about conflicting interests (see, for example, the Justice Select Committee's examination of the Information Commissioner's independence and budget, which recommends that body should report to, and be funded by Parliament).[58] In light of the significance of the role to be played by the IPC, and the very substantial overlap between its scrutiny function and the work of the Secretary of State, there is, in our view, a strong case for a different funding model.

61. In any event, given that Judicial Commissioners will be drawn from the pool of judicial expertise and may be former – or sitting – senior judges, the judiciary or Her Majesty's Courts and Tribunals Service should be involved in or consulted about budget setting for the IPC. Importantly, if a number of judges are to be drawn away from the High Court to sit as part of the IPC, this reduces the capacity of the High Court which should accordingly be compensated by the Treasury to maintain its capacity. Judicial Commissioners should not be appointed at cost to the wider judicial system.

(ii) Independent and effective?

62. We are concerned that the Bill replicates the language and model adopted by RIPA, focusing on the "Commissioner" rather than the Commission. This may appear a superficial distinction, but the structure of the Commission may be crucial to its success in practice. Not least, it appears from the face of the Bill that the Government intends to conflate the judicial and the inspection and audit functions of the Commission within the responsibilities of the Judicial Commissioners.

63. Clause 169 sets out the main oversight functions of the "Commissioners". In Clause 169, the Draft Bill places a broad duty on Judicial Commissioners not to act in a manner which

[57] Q 56, HC 651, 2 December 2015.
[58] See Ninth Report of 2012-13, *The functions, powers and resources of the Information Commissioner,* paras 28 – 31.

is contrary to the public interest or prejudicial to national security, the prevention and detection of crime or the economic well-being of the United Kingdom. We regret the inclusion of this duty in the Draft Bill. It appears, at best, superfluous, in light of the functions of the IPC, and at worst designed to encourage a degree of deference within the Commission towards the assessment of the Secretary of State and individual agencies and bodies of the risks associated with their work. However, that this Clause distinguishes between warranting (where the duty will not apply) and the wider functions of the Commissioners suggests that the Commissioners will be undertaking both judicial and audit functions.

64. Plainly, the credibility of the Judicial Commissioners may be reduced if they appear to be "checking their own homework". The conflation of the judicial and inspection roles within the Commission is inappropriate, reduces the objective independence of the Judicial Commissioners and could undermine the effectiveness of the IPC model.

65. In *Freedom from Suspicion: Building a surveillance framework for a digital age,* we explained our view that:

> *"There are plainly considerable advantages to all the relevant expertise being combined within a single body, and the involvement of judicial commissioners will go a long way towards helping to establish its institutional independence. As for the concern about combining authorisation and oversight within a single body, we do not see grounds for particular concern. As the Independent Reviewer noted, the Office of the Chief Surveillance Commissioner already performs authorisation and oversight functions in respect of Part 2 of RIPA[59] and there has been no criticism of that model that we are aware of. On the contrary, we consider that there are likely to be significant benefits from having a pool of judges with expertise in surveillance matters, supported by an independent body with the high level of technical and cross-disciplinary expertise that will be necessary to provide effective scrutiny in this fast-changing field."*[60]

66. Our view is based on the consideration that, within a single organisation, the judicial and audit functions within the body would remain operationally distinct (See Annex 17, Anderson Review, for example). While the Judicial Commissioners would benefit substantially from being able to draw upon the technical expertise open to inspectors and auditors, we are concerned that the conflation of roles in the Draft Bill would undermine both judicial independence and public confidence in the IPC. If their functional independence cannot be maintained within the IPC model, another structure may be more appropriate.

[59] *Anderson Review*, para 14.98.
[60] *Freedom from Suspicion: Second Report,* para 47.

67. In the interests of maintaining the independence of the Commission, the Investigatory Powers Commissioner and the Judicial Commissioners should be subject to an appointment mechanism which is beyond reproach. We are concerned that the Draft Bill provides for an appointment by the Prime Minister alone, although the IPC should be consulted. At the very least, we would expect the Lord Chief Justice to be involved in, or consulted on, a judicial appointment of this nature. However, we recommend that each of these appointments is made by the Judicial Appointments Commission ('JAC'). While we welcome the provision in the Bill for these appointments to be drawn from those who have already held high judicial office; we consider that suitability for appointment *to these particular posts* should be tested in an open and transparent way, best managed by the JAC.

(iii) Powers and responsibilities

68. Clause 169 of the Draft Bill sets out the main oversight functions of the Investigatory Powers Commissioner. Clause 169(1)-(3) creates a very broad duty to keep "under review" the exercise by public authorities of various statutory functions under this Bill and under RIPA, the Police Act 1997 and the Intelligence Services Act 1994. This reviewing power will "include" "audit, inspection and investigation".

69. On 2 November 2015, following a roundtable conducted by JUSTICE and King's College London, the Interception of Communications Commissioners Office ('IOCCO') produced a "wish-list" for any new single body.[61] These included the power to conduct investigations and thematic inquiries at their own instigation and the power to refer specific cases to the IPT for determination. This reflects our recommendations in *Freedom from Suspicion* that any consolidated body should be able to refer cases directly to the IPT and that the oversight of surveillance should be designed to address thematic problems and to provide for more wide-ranging inquiries about the effectiveness of the law.[62]

70. The Draft Bill should be amended to put beyond doubt the capacity of the IPC to conduct inquiries on its own initiative about the operation of the legal framework within its sphere of responsibility. While this power might be used sparingly within the resources available,

[61] http://www.iocco-uk.info/docs/Kings%20College%20Round%20Table.pdf
[62] Although in our first report, we recommended that the IPT should adopt responsibility for these more thematic inquiries, it would be entirely proper for the new IPC to have this inquisitorial role.

it could be extremely effective in identifying good practice and areas where the law remains uncertain. We return to the relationship between the IPC and the IPT, below.

71. Section 170 creates a power for the Prime Minister to direct the IPC to conduct a review of any aspect of the functions of the intelligence services, the head of any such service or any part of the armed forces or MoD in so far as they are conducting intelligence activities. It is unclear how this power is intended to be exercised and how far this kind of investigation might be designed to replace or supplement inquiries by the Intelligence and Security Committee or public inquiries into matters of public importance relating to the conduct of the intelligence services or the armed forces. As the Bill provides for the scope of such inquiry to be determined by the Prime Minister, who is also permitted to redact any conclusions of an inquiry by the IPC, its output may be of limited value for the purposes of meeting any responsibility on the part of the Government to conduct an independent, effective and transparent inquiry (including, for example, in connection with an Article 2 ECHR obligation in any case where deaths have resulted).

72. Clause 172 stipulates particular duties for the Judicial Commissioners in connection with the work of the IPT. This includes providing assistance and advice to public bodies and others within their sphere of responsibility and to the IPT, including on cases live before the Tribunal (echoing Recommendation 117 of the Anderson Review). We welcome the acknowledgment that the Commissioners and the IPC might have a role in providing advice or guidance on the application of the law. However, the Committee may wish to consider whether the relationship between the IPC and the IPT is properly drawn. The IPT may ultimately take decisions on the lawfulness of decisions by the Commissioners. We are particularly concerned that, in any circumstances where the Judicial Commissioners are giving their view on the law, they may be required to first consult with the Secretary of State (Clause 172(3)). This could undermine the apparent independence of the Judicial Commissioners.

73. The Draft Bill makes no provision, beyond error notification (see below), for the IPC to refer an issue directly to the IPT. In circumstances where apparently unlawful conduct is identified in the course of an investigation or an audit, or inconsistency in the application of the law, it may be helpful for the IPC to refer an issue directly to the IPT. This could be particularly useful where an issue affects a group or class of individuals unlikely to pursue an individual claim before the Tribunal; or in circumstances where the interpretation of the law or its application to a new practice may be in doubt.

74. Finally, we regret the very broad provision for the functions and powers of the IPC to be amended by Ministers in secondary legislation (Clause 171(9)). The limited capacity for Parliamentary scrutiny of secondary legislation makes this power inappropriate. The existence of this power endangers the apparent independence of the Commission and its effectiveness as a safeguard against abuse.

(iv) Notice and redress

75. Clause 171 provides a mechanism for the IPC to report errors to the IPT. The IPC must report to the subject of any surveillance any "relevant error" which it considers is a "serious error". The individual will only be informed if the IPT agrees it is a "serious error" and it is in the public interest for the person concerned to be informed.

76. While we recommended in *Freedom from Suspicion* that errors should be notified to the IPT and the individual concerned, there are a number of significant problems with this measure:

a. We understand that, in practice, IOCCO already reports errors relating to communications data where relevant, in which case, this provision would constrain existing practice through the addition of new qualifiers and limitations on reporting. The Draft Bill includes an express bar on reporting of any other errors except by virtue of Clause 171 (Clause 171(9));
b. The Draft Bill defines the seriousness of any error by reference to the impact on the individual concerned, without reference to the illegality of the conduct by the relevant public body. Any reportable error must, in the view of the Commissioner, have caused "significant prejudice or harm to the person concerned" (Clause 171(3)). This would significantly limit the circumstances when the duty to report is triggered, despite unlawful conduct by a public body inspected by the IPC.
c. This "serious error" benchmark is set disproportionately – and inappropriately – high by the Draft Bill. Clause 171(4) indicates that something *more* than a breach of Convention rights protected by the HRA 1998 is required for an error to be considered "serious".
d. If the purpose of reporting is to allow an individual to consider whether to pursue a case before the IPT, it is unclear why reports should be limited only to cases of serious error. The Bill provides a detailed mechanism for reporting on serious errors and the maintenance of relevant data about reported errors (Clause 171(10)). We are concerned that the distinction between serious and other errors

could, in practice, lead to underreporting of surveillance inconsistent with the requirements of the law or the relevant Codes of Practice. This could significantly diminish the effectiveness and value of the new IPC.

77. This provision falls far short of the mandatory notification requirements which operate in other countries. The Bill should be amended to give the IPC a duty to notify any relevant person of any error discovered in targeted surveillance, except in circumstances where disclosure would risk any on-going operation or investigation, or otherwise endanger national security or the prevention and detection of crime.

78. We consider that the Draft Bill should additionally be amended to provide for a *default* mandatory notification mechanism.[63] The requirement for individuals to be notified of surveillance as soon as possible, is a key safeguard identified by the European Court of Human Rights, which as stressed that *"as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned".*[64] The House of Lords Constitution Committee has previously recommended that *"individuals who have been made the subject of surveillance be informed of that surveillance, when completed, where no investigation might be prejudiced as a result".*

79. Provision for mandatory notice would allow individuals to pursue a claim before the IPT in their own right even in circumstances where the IPC has not identified an error. This model operates in other countries without difficulty, and although notification in very sensitive cases may be less likely, the potential for disclosure may create an additional impetus towards lawful decision making by agencies and other bodies exercising these compulsory powers. For example, for instances of interception in law enforcement matters in the United States, notification is by default within 90 days of the termination of the relevant surveillance, unless the authorities can show there is "good cause" to withhold that information.[65] A similar model operates in Canada, where the subjects of interception warrants for the purposes of law enforcement must be given notice within 90 days of a warrant expiring. This may be extended up to three years in terrorism claims, subject to judicial oversight, if in the "interests of justice".[66] We understand that similar

[63] *Freedom from Suspicion,* para 389.
[64] See *Association for European Integration and Human Rights and Ekimhzhiev* App No 62540/00, 28 June 2007, para [90]-[91
[65] 18 U.S.C §2518 (8) (d). See Annex 15, Anderson Review, for a brief analysis of comparative practice in the "five eyes" jurisdictions.
[66] Section 188, 195-196, Canadian Criminal Code.

models apply in both Germany and the Netherlands, with similar exemptions to protect the integrity of ongoing inquiries.[67]

(v) Disclosure, cooperation and whistle-blowing

80. While we welcome a number of measures in the Draft Bill designed to protect against abuse of power, we are concerned that prohibitions on disclosure should not inadvertently discourage or prevent individuals within public authorities or agencies or in CSPs from approaching the IPC with concerns or communicating with the Commission frankly.

81. Notably, Clause 8 provides for an offence of unlawfully obtaining communications data. Clause 43 prevents individuals from disclosing whether an intercept warrant is in place, or its terms. Clause 66 makes it an offence for telecommunications operators or their employees to disclose any information about the requirements imposed on them in connection with communications data or access to that data. Although Clause 43 makes provision for an authorised disclosure to a "Judicial Commissioner", this exception is not consistently applied to all non-disclosure duties and offences in the Bill. (We address our concerns about the scope of the role of the Judicial Commissioner, above).

82. In light of the history of significant misunderstandings and disagreements about the scope of surveillance law, it would be regrettable if individuals and organisations were prevented from consulting with the IPC about good practice and legality by overly rigid non-disclosure requirements. It must be open to individuals – in either public bodies or CSPs – to ask the IPC for guidance and draw their attention to areas of conflict in the application of the law. This might be particularly helpful where there is a disagreement between different public bodies, or between a CSP and a public agency, about the precise scope of the powers circumscribed. Similarly, a safe-route to the IPT for would-be whistle-blowers wishing to report bad practice should be clear and accessible. This could be achieved by inserting a provision into Part 8 specifying that any disclosure to the

[67] Under the German Code of Criminal Procedure, section 101(4)(3), individuals under telecommunication surveillance shall be notified of surveillance measures. The notification should mention the individual's option of court relief and the applicable time limits and should be given as soon as possible without "endangering the purpose of the investigation, the life, physical integrity and personal liberty of another or significant assets including the possibility of continued use of the undercover investigator." But notification will be "dispensed with where overriding interests of an affected person that merit protection constitute an obstacle." In the Netherlands, under the Code of Criminal Procedure, Part VD, Chapter One, Section 126bb, the public prosecutor must notify in writing the user of telecommunications or the technical devices of the surveillance "as soon as the interest of the investigation permits", but not if it is not reasonably possible to do so. If the individual is a suspect and learns of the exercise of surveillance power through means described in 126aa(1) or (4) of the Code, notice is not required. If the inquiry relates to an investigation of terrorist offences or another serious offence, information pertaining to an individual's name, address, postal code, town, number, and type of service of a user of a communication service may be requested, and the notice provisions of 126bb will not apply.

IPC for the purposes of soliciting advice about any matter within the scope of its responsibilities, or for the purposes of supporting its duty to review, will be an authorised disclosure, not subject to any criminal penalty.

(f) The Investigatory Powers Tribunal

83. Four years ago, we regretted the difficulty of bringing a claim before the Investigatory Powers Tribunal ('IPT') and the limited form of redress available before the Tribunal. We made a series of recommendations concerning the role of the IPT:

    a. oversight commissioners should have the power to refer cases to the IPT for investigation whenever he or she reasonably suspects that a public authority has acted unlawfully, including the unnecessary and disproportionate use of surveillance powers;[68]

    b. mandatory notification periods should be specified in law (see above);[69]

    c. the investigative capabilities of the Tribunal should be increased and extended to enable it to undertake proactive investigations arising from any systemic failings identified by the relevant oversight commissioner, or in cases where there are reasonable grounds to suspect the unauthorised use of surveillance by a public body;[70]

    d. the Tribunal should adopt internal procedures to increase adversarial testing of relevant evidence, including the appointment of a standing panel of special advocates to represent the interests of the excluded party in any case where the Tribunal's investigations have identified a case to be answered;[71] and

    e. the existing policy of Neither Confirm Nor Deny ('NCND') should be relaxed sufficiently to enable the Tribunal to adopt fair procedures (including the right to an oral hearing, disclosure of evidence, cross examination of witnesses and the giving of reasons).[72]

[68] *Freedom from Suspicion*, para 397.
[69] *Freedom from Suspicion,* para 396.
[70] *Freedom from Suspicion*, para 398.
[71] *Freedom from Suspicion*, para 399.
[72] *Freedom from Suspicion*, para 400. Since our recommendation in 2011, we note that the doctrine of NCND has come under some judicial criticism in recent years: see e.g. the speech of Maurice Kay LJ in *Mohamed Ahmed Mohamed and CF v Secretary of State for the Home Department* [2014] EWCA Civ 559 at para 20 ("It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it") and that of Bean J in *DIL and others v*

84. In the wake of the Snowden disclosures, the IPT considered a number of complaints concerning the activities of the intelligence services. In addition, complaints have been brought concerning the use of surveillance powers to identify journalists' sources. In 2015, the IPT delivered no less than three judgments identifying a breach of Convention rights:

    a. In *Liberty and others v GCHQ and others (No 2),*[73] the Tribunal held that, prior to its disclosure of the relevant internal arrangements for the handling of such material, the legal regime governing the intelligence services' receipt of communications intercepted by foreign intelligence services had not complied with the requirements of legal certainty under Articles 8 and 10 ECHR;

    b. In *Belhaj and others v Security Service and others*,[74] the IPT held that the legal regime governing the interception of legally privileged material was not in accordance with the law under Article 8(2) ECHR; and

    c. In *Liberty and others v GCHQ and others (No 3)*,[75] the IPT held GCHQ's interception of the private communications of two human rights organisations – the Egyptian Initiative for Personal Rights and the Legal Resources Centre – had violated their rights under Articles 8 and 10 ECHR. Several days later, however, the Tribunal notified the parties via email that it had made a mistake in its determination, and that it was Amnesty International and not the Egyptian Initiative that had been the victim of unlawful interception.

85. In the first instance, the three cases show the importance of notification of surveillance. In our 2011 report, we noted that it was no coincidence that half the successful complaints to the IPT involved cases where the complainants had been notified that they had been subject to surveillance. So too in the cases of *Liberty and others* and *Belhaj*, but for the disclosure of Edward Snowden as to the activities of the UK's intelligence services, the complaints would never have been brought and the public at large would have had no inkling that the legal framework was not compatible with the requirements of the Convention.

Commissioner of Police of the Metropolis [2014] EWHC 2184 (QB) para 42 ("just as (in the well-known words of Page Wood V-C in *Gartside v Outram* (1856) 26 L.J.Ch 113) "there is no confidence as to the disclosure of iniquity", so there can be no public policy reason to permit the police neither to confirm nor deny whether an illegitimate or arguably illegitimate operational method has been used as a tactic in the past").

[73] [2015] UKIPTrib 13_77-H, 6 February 2015.

[74] [2015] UKIPTrib 13_132-H, 13 March 2015.

[75] [2015] UKIPTrib 13_77-H_2, 22 June 2015.

86. In its recent report, the ISC praised the Tribunal as "*an important component of the accountability structure*" but recommended the introduction of a domestic right of appeal against its decisions.[76] The RUSI panel described the Tribunal as "*a work in progress*" and made several criticisms of its procedures, including that the Commissioners have no power to refer cases to the Tribunal;[77] secondly, that its rulings were frequently "*opaque*";[78] that its reliance on complaints brought by the public "*was not a helpful or just arrangement*";[79] and that its recent confusion between Amnesty International and the Egyptian Initiative for Personal Rights pointed to the need for "*clear procedural improvements that will need to be implemented*".[80] It also endorsed the need for a domestic right of appeal.[81]

87. For his part, the Independent Reviewer noted that the Tribunal was operating increasingly in the open and was "*likely increasingly to be perceived as a valuable and effective check on the exercise of intrusive powers*".[82] He supported the introduction of a right of appeal on points of law and changes to enable the IPT to make declarations of incompatibility pursuant to Section 4, HRA 1998.[83] Notably, the Independent Reviewer declined to make any recommendations concerning the Tribunal's procedures, indicating that this was an issue for argument on "another day" (outside the scope of his inquiry).[84]

(i) Appeal rights

88. Clause 180 introduces a right of appeal from the IPT "on a point of law", subject to certification by the IPT or the appropriate appeal court. JUSTICE welcomes the introduction of this right of appeal. We are concerned however that it appears that the Draft Bill would only provide for appeals against a final *determination*, not in respect of interim legal findings during the conduct of the proceedings. This could lead to unfairness and wasted resources as proceedings may continue to a full determination, on the basis of an error in law, only to result in an appeal at a later stage.

89. Clause 180 provides that the route of appeal will be determined by the Secretary of State in regulations, with such cases as determined to be heard by a specified court in

[76] *ISC Report*, para 217LL.
[77] *RUSI Report*, para 4.87.
[78] Ibid, para 4.89.
[79] Ibid, para 4.88.
[80] Ibid, para 4.94.
[81] Ibid, para 4.86.
[82] *Anderson Review*, para 14.102.
[83] *Anderson Review*, recommendation 114 and para 14.105.
[84] *Anderson Review*, para 14.108.

Scotland or Northern Ireland, or in other cases by the Court of Appeal. JUSTICE considers that delegation of this kind is inappropriate. Routes of appeal should be specified on the face of the Bill.

(ii) IPT and procedural reform

90. JUSTICE regrets that the Draft Bill takes no further steps to increase the openness and effectiveness of the IPT and the ability of individuals to secure redress for unlawful acts of public surveillance. We consider this a missed opportunity:

a. **Notification:** We consider the limited provision for notification in the Draft Bill, above. We consider that a default statutory framework for the after-the-event notification of individuals subject to surveillance would significantly improve the likelihood that individuals are able to pursue their claims before the IPT. As explained above, while the IPT has worked hard during the past year to eighteen months, the bulk of this work as arisen as a result of the Snowden revelations. Without the objects of surveillance having knowledge that a claim may be appropriate, it is unlikely that the workload of the Tribunal will be sustained.

b. **Procedures and openness:** Like the Independent Reviewer, we welcome the Tribunal's recent efforts to improve the transparency of its procedures. Those efforts, however, remain very much bound by the constraints imposed by RIPA and the Tribunal's ability to set its own procedural rules. The Committee has received direct evidence from others, including Amnesty International, on the opaque nature of proceedings in the Tribunal. Nothing in the Draft Bill would address the inherent limitations in the procedures before the IPT.

In light of the consensus across each of the three reviews – ISC, Anderson and RUSI – towards greater openness before the IPT, we recommend that the Draft Bill is amended to provide that all proceedings before the IPT should be open, unless a closed material procedure can be justified in the public interest.

This approach would test the boundaries of the blanket "*Neither Confirm nor Deny*" ('NCND') principle. Although the Tribunal has found a means to work around the application of NCND, by proceeding on the basis of assumed facts, the limitations of this approach have become apparent during the course of the preparation of the Draft Bill. In the litigation preceding the introduction of the Bill,

the Government has incurred significant litigation costs refusing to confirm, nor deny, certain practices by the security agencies, which have now been avowed in connection with the passage of this Bill (some as late as in the material accompanying its publication).[85]

c. **Adversarial testing/Special advocates:** JUSTICE considers that the Bill should be amended to make clear that in any closed session, a Special Advocate is appointed to allow any case to be subject to adversarial testing. However valuable the role played by counsel to the Tribunal in closed proceedings, it is not an effective substitute because counsel to the Tribunal is *not* charged with representing the interests of the excluded party and, in the *Liberty* case, counsel took no instructions from the excluded parties.

Parliament should take this opportunity to specify – whether in the model of a Special Advocate - or through an express obligation to appoint a Counsel to the Tribunal – that any claimant's interests should be represented in closed session by a security vetted counsel and the case of the public agency concerned subject to adversarial scrutiny.

While JUSTICE has principled concerns over the expansion of the use of secret evidence, such limited scrutiny and representation offered by a Special Advocate should not be limited to the discretion of any individual court, but available as of right in any case involving a closed material proceeding, including before the IPT.[86]

d. **Human Rights Act 1998:** The Bill should be amended to implement the Anderson Review recommendation that the IPT should be empowered to make a declaration of incompatibility pursuant to Section 4, HRA 1998. While the right to appeal will ensure that a declaration might be sought before the Court of Appeal, the Tribunal should have the opportunity to consider whether a declaration would be appropriate. It would be an inefficient use of judicial resources if the only reason an appeal might be pursued would be to secure a remedy unavailable at first instance.

[85] See *Freedom from Suspicion,* 392 – 393, *Freedom from Suspicion: Second Report,* paras 39 – 40.
[86] See *Freedom from Suspicion,* para 378 – 392; *Freedom from Suspicion: Second Report,* para 41.

(g) Privileges

91. JUSTICE is concerned that the treatment of important legal privileges, and notably, legal professional privilege, in the Bill is cursory. The Bill provides that where the correspondence of Members of Parliament (or Members of the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly) is subject to targeted interception or a request for access to communications data, the Secretary of State must consult the Prime Minister before granting the relevant warrant (Clauses 16 and 85). Clause 61 provides that access to communications data *for the purpose of* targeting journalistic sources must be authorised by a Judicial Commissioner. The only reference to legal professional privilege is in Schedule 6, which provides that the Code of Practice on Communications Data will make provision for any particular considerations relevant to legally privileged information (Schedule 6 (4)).

92. In *Freedom from Suspicion,* JUSTICE regretted that the treatment of legal professional privilege under RIPA had been inadequate and that the Codes of Practice produced under its various parts had provided little reassurance to the public that communications which benefitted from privilege were being handled lawfully.[87] In the interim, domestic court decisions have confirmed that the treatment of privileged material under the RIPA framework has been far from certain either for the agencies or the beneficiaries of the relevant privileges.[88]

(i) Legal Professional Privilege

93. JUSTICE shares the concerns expressed by the Bar Council, the Law Society of England and Wales and others, that in order to afford proper respect to legally privileged material, the Draft Bill must be amended.[89]

94. Legal professional privilege is a core principle at the heart of any effective justice system, designed to preserve access to justice and the rule of law. By ensuring that individuals are able to take legal advice in confidence, without fear of interference, the rule preserves the right of persons to access the law fully and fairly. This principle is one respected in

[87] *Freedom from Suspicion,* paras 110 – 115, 339 – 342.
[88] See, for example, *Belhadj,* [2015] UKIP Trib 13_132-H, *Lucas, Jones and Galloway v SSHD & Ors,* [2015] UKIPTrib 14_79-CH. See also, *R v Barkshre* [2011] EWCA Crim 1885.
[89] See, for example, Draft Investigatory Powers Bill, Parliamentary Briefing, Bar Council, November 2015; Investigatory Powers and Legal Professional Privilege, Bar Council, Faculty of Advocates, The Bar of Northern Ireland and The Law Society of England and Wales, October 2015; and Response to the Joint Committee on the Draft Investigatory Powers Bill, The Odysseus Trust (Office of Lord Lester of Herne Hill QC), 15 December 2015.

democratic countries the world over. It rightly exists to protect the rights of the client, not the interests of the legal professional. Thus, privilege can only be waived with the consent of a client. The European Court of Human Rights has stressed that surveillance measures which might endanger professional privilege will require additional safeguards.[90] Each of the three reports – ISC, Anderson and RUSI – recognise the importance of privileges and confidence in connection with surveillance powers.[91]

95. The material which accompanies the Bill explains the Government's view that the Part 3 Code of Practice, dealing with communications data, will require applicants for a warrant seeking access to data containing legally privileged material to provide a "compelling case".

96. JUSTICE considers that this approach falls far short of the provision necessary to preserve client confidence in legal professional privilege:

    a. Codes of Practice are subject to limited Parliamentary scrutiny. Although they might be approved by Parliament, as delegate legislation, they are unlikely to be subject to detailed debate, and MPs and Peers will have no opportunity to provide for their amendment;

    b. The existing Codes have proved an unsatisfactory bulwark against abuse (see *Belhadj* (IPT). The revised versions are also likely to provide a similarly limited safeguard;[92]

    c. While Draft Codes are unavailable for review, any model which permits surveillance of legally privileged material would be overbroad and inconsistent with the spirit of the existing case law.

    Although the House of Lords accepted that RIPA might permit the interception of legally privileged materials in *Re McE,* the conclusions in that case are limited and controversial. In light of the long standing protection for legal professional privilege offered in centuries of common law, and in statute (for example, in the Police and Criminal Evidence Act 1984), the decision was a surprise to

[90] *Niemietz v Germany* [1992] 16 EHRR 97; *Kopp v Switzerland* App No 23224/94.
[91] *ISC Report*, Chapter 10(d), p95; *Anderson Review*, para 2.12, *RUSI Review*, para 2.10.
[92] Notably, these Codes proceed on the basis that interference with legally privileged material is authorised by RIPA. See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473845/6.1276_151104_INTERCEPTION_CoP_for_designer_FINAL_WEB.PDF. This Code was laid before Parliament on 4 November 2015; at the time of writing it was not yet approved.

practitioners and commentators alike. The case considered an analysis of a part of RIPA which did not expressly mention legal professional privilege, nor which Parliament had considered. In any event, the decision should be narrowly confined to truly exceptional circumstances and subject to the highest possible safeguards. For example, Lord Carswell considered "grave and imminent threats" alone, such as the killing of a child or an imminent terror attack, might justify interference with legal privilege.[93] Equally, Lord Phillips indicated the importance of prior judicial authorisation, indicating that the European Court of Human Rights would require at a minimum that interference with privileged material should be governed by a clear statutory framework, providing the limited circumstances where privilege might be overridden and access to person with "judicial status" to determine any such question.[94]

It is clear that the Draft Bill contains no such limitations.

d. The approach in the Draft Bill would offer *less* protection to legally privileged material than to the protection of journalistic sources or to the communications of Members of Parliament. Of all the privileges considered in connection with the Draft Bill, the case for the protection of legally privileged material is beyond question. That it is the only privilege not afforded specific protection on the face of the Draft Bill is regrettable.

97. Broadly, in our view:

a. The Bill must acknowledge that the protection of legal professional privilege is important for *all* forms of surveillance, including bulk forms of activity.

The Draft Bill currently confines its provision to the treatment of communications data. It makes no mention of the privilege in connection with retention of data; or methods which might in practice be *more* intrusive, including targeted interception warrants and forms of equipment interference.

b. There should be a clear statutory presumption that legally privileged material should not be deliberately targeted for surveillance. This should only apply to material which attracts privilege. Where privilege is lost or set aside, including in

[93] See *Re McE* [2009] 1 AC 908, [108]
[94] See *Re McE* [2009] 1 AC 908, [41]

circumstances where a lawyer is complicit in unlawful behaviour ('the iniquity exemption'),[95] the bar should not apply.

c. If there are any circumstances where material which might be legally privileged may be sought (e.g. in reliance on the 'iniquity principle'), this should be subject to clear prior judicial authorisation, not Ministerial or official authorisation subject to subsequent judicial review (see above).

d. Codes of Practice for each of the powers granted in the final Bill should be required to provide guidance to prevent, in so far as possible, the inadvertent capture of legally privileged material, and to ensure that if captured, such data is afforded such additional protection as necessary to ensure respect for access to justice and the rule of law. The Bill should be redrafted to specify that the purpose of any guidance in the Code should be designed to protect against the unlawful disclosure of privileged material.

(ii) The 'Wilson' Privilege/Journalistic sources

98. JUSTICE considers that the other privileges in the Bill should be subject to a similarly comprehensive approach. We are concerned about the inconsistency of approach in the Draft Bill. Thus, additional protection is afforded to Members of Parliament subject to a targeted interception warrant, but not to journalists seeking to protect their sources. Similarly, while access to communications data which targets journalistic sources provides for authorisations to be subject to judicial review, access to other communications data, which might engage the privilege afforded to Members of Parliament or to legally privileged material is not.

99. There are some wider concerns about these provisions, which the Committee might wish to consider. For example, will consultation with the Prime Minister provide significant reassurance for members of parties in opposition? Similarly, will such consultation garner much reassurance outside Westminster, if at all? In considering the sanctity of communications with members of the Scottish Parliament and the Welsh and Northern Ireland Assemblies, members might with to consider whether consultation with the Prime Minister would give any comfort.

[95] See for example, Police and Criminal Evidence Act 1984, Section 10(2). Importantly, it appears that the Government does not seek to target LPP, but only the circumstances when it may be abused. If this is the case, then there should be no objection to amendment of the Draft Bill to exclude deliberate targeting of legally privileged material in applications, as abuse of the kind envisaged would abrogate the privilege concerned. See 30 November 2015, Evidence of Paul Lincoln, Q 15, HC 651, 30 November 2015.

100. The Committee may wish to ask the Government to explain the inconsistency in approach to each of the privileges considered in the Draft Bill, and to explain a) why the safeguards afforded to each might differ; b) why those safeguards might be different for different kinds of surveillance; and c) why the protection offered should not be specifically determined by Parliament on the face of the Bill.

(h) Intercept as evidence

101. Clause 42 of the Draft Bill, together with Schedule 3, broadly replicates the existing procedure in Section 17(1) of RIPA, whereby material obtained by way of an intercept warrant cannot be used as evidence in ordinary criminal proceedings. Schedule 3 makes a number of exceptions to allow intercept evidence to be considered in civil proceedings where a closed material procedure – where a party and his or her legal team are excluded – is in place. These proceedings, for example, include proceedings under Section 6 of the Justice and Security Act 2015, in the Special Immigration Appeals Commission or under the Terrorism Prevention and Investigation Measures Act 2011. There is no exemption for criminal proceedings, except in so far as material may be disclosed to the prosecution and to the judge, in order that a judge might determine whether admissions by the Crown are necessary in order for the trial to proceed in a manner which is fair; (if it would not be fair, a prosecution may have to be dropped).[96]

102. JUSTICE has long recommended the lifting of the bar on the admission of intercept material as evidence in civil and criminal proceedings. In 2006, we published *Intercept Evidence: Lifting the ban,* in which we argued that the statutory bar on the use of intercept as evidence was 'archaic, unnecessary and counterproductive'.[97] The UK's ban reflects a long-standing Government practice but it is out of step with the position in many other commonwealth and European countries and it has proved increasingly controversial over time. Importantly, the ECtHR has recognised the value placed on admissible intercept material, in countries where it is available, constitutes 'an important safeguard; against arbitrary and unlawful surveillance, as material obtained unlawfully will not be available to found the basis of any prosecution.[98] In 2014, a Privy Council review

[96] See Schedule 3(21).
[97] See JUSTICE, *Intercept Evidence: Lifting the ban*, October 2006, p13 – 17. See also *Freedom from Suspicion,* paras 129 – 139.
[98] *Uzun v Germany,* App No 35623/05, [72].

confirmed that fully funded model for the removal of the ban could result in a "significant increase in the number of successful prosecutions".[99]

103. The Targeted Intercept Factsheet produced by the Government to accompany the Draft Bill, states:

> *"Intercept material cannot be used as evidence in criminal proceedings. Successive Governments have reviewed whether it would be possible to introduce intercept as evidence. Each has concluded that it would not be possible - the Agencies' abilities to conduct the investigations that we rely on to keep us safe would diminish."* [100]

104. This reflects the position in the latest Privy Council review, which concludes that complying with existing disclosure requirements and preparation for trial would be administratively difficult and costly. Since the precise benefit in increased successful prosecutions cannot be quantified, there will be no change in position unless law enforcement budgets could be increased:

> *"the increased resource burden would mean either that a very large amount of other agency activity was dropped to fund intercept as evidence or that interception would be available for many fewer investigations or both."*[101]

105. David Anderson QC considered that the ban on intercept evidence was not within the remit of his review. He did, however, note that "*the relative impact of interception is probably in decline, as communications data become more abundant*". He acknowledged CPS evidence that the bar on intercept material meant that communications data was of increasing importance in securing prosecutions.[102]

106. As our 2006 report made clear, the experience of other countries shows that the fears of the intelligence services about the operational impact of using intercept as evidence is ill-founded. Intercept evidence has been admissible for many years in such common law countries as Australia, Canada, New Zealand, South Africa and the United States. Not only do all these countries share the same adversarial legal system as our own, but they have similar disclosure requirements to those required in England and Wales.[103]

---

[99] *Intercept as Evidence*, Cm 8989, December 2014, para 84. The review also reflected the concerns of the agencies and law enforcement bodies that removing the ban without full funding could reduce their effectiveness.
[100] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473739/Factsheet-Targeted_Interception.pdf
[101] *Intercept as Evidence,* Cm 8989, December 2014, paras 86 - 91.
[102] *Anderson Review*, para 9.16 – 9.18.
[103] *Freedom from Suspicion,* para 138.

107. The failure of this Bill to reconsider the role of intercept material as evidence would represent a missed opportunity for Parliament to bring UK practice into line with the approach in other countries; a step which consensus agrees could lead to more successful prosecutions against those guilty of terrorist offences and other forms of serious crime. The Committee may wish to consider how the bar on the use of targeted intercept material relates to a new focus on expanded and untargeted access to communications data; and whether lifting the ban (a) would increase the likelihood of successful criminal prosecutions, (b) would reduce reliance on administrative alternatives to prosecution, such as Terrorism Prevention and Investigation Measures Orders ('TPIMs') or on the use of untargeted forms of surveillance, and (c) whether the costs based analysis conducted by the Government is accurate and sustainable.

JUSTICE

December 2015