Freedom from Suspicion:

Building a Surveillance Framework for a Digital Age.

A report by JUSTICE

About JUSTICE

Established in 1957 by a group of leading jurists, JUSTICE is an all-party law reform and human rights organisation working to strengthen the justice system – administrative, civil and criminal – in the United Kingdom. We are a membership organisation, composed largely of legal professionals, ranging from law students to the senior judiciary.

Our vision is of fair, accessible and efficient legal processes, in which the individual's rights are protected, and which reflect the country's international reputation for upholding and promoting the rule of law. To this end:

- We carry out research and analysis to generate, develop and evaluate ideas for law reform, drawing on the experience and insights of our members.
- We intervene in superior domestic and international courts, sharing our legal research, analysis and arguments to promote strong and effective judgments.
- We promote a better understanding of the fair administration of justice among political decision makers and public servants.
- We bring people together to discuss critical issues relating to the justice system, and to provide a thoughtful legal framework to inform policy debate.

A key goal is to provide evidence-based analysis to inform the development of new law and policy and to propose practical solutions to legal problems for lawmakers, judges and public servants.

Contents

Summary

"Surveillance is a necessary activity in the fight against serious crime. It is a vital part of our national security. Unnecessary and excessive surveillance, however, destroys our privacy and blights our freedoms.

The Regulation of Investigatory Powers Act 2000 is neither forward-looking nor human rights compliant. Piecemeal amendments are no longer enough for what is already a piecemeal Act. Root and branch reform of the law on surveillance is needed to provide freedom from suspicion, and put in place truly effective safeguards against the abuse of what are necessary powers."

JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (2011)

In 2011, JUSTICE published *Freedom from Suspicion: Surveillance Reform for a Digital Age*, a considered report on the failure of the surveillance framework in the UK to keep pace with changing technology, to the detriment of both individual privacy and the credibility of the work of our law enforcement and intelligence agencies. We recommended that the law be rewritten to provide a new legal framework, containing adequate safeguards and setting new standards for a digital age.

Developments in the past four years have confirmed that reform is not only timely, but crucial. From the scrapping of the draft Communications Data Bill in 2012 and the revelations of Edward Snowden in 2013 about the retention of data sent by UK citizens using overseas providers, to the passage of the Data Retention and Investigatory Powers Act in 2014, the shortcomings of the Regulation of Investigatory Powers Act 2000 have been well illustrated.

Following detailed reports recommending reform, from the Intelligence and Security Committee, the Royal United Services Institute and the Independent Reviewer of Terrorism Legislation, the case for change is robust.

The Government plan to introduce a new draft Investigatory Powers Bill with consideration of a new legislative framework by Parliament in 2016.

JUSTICE continues to support the development of a surveillance framework consistent with our recommendations in Freedom from Suspicion. In this report, we focus on authorisation of surveillance decision making, the role of the Investigatory Powers Tribunal and oversight and accountability.

The existing law has failed. Rebuilding provides a vital opportunity to create a law which is transparent and clear and which has at its heart strong safeguards to protect the rights of the individual and preserve the credibility of law enforcement and intelligence agencies. A law truly fit for a digital age.

Recommendations

Authorisation and surveillance

- JUSTICE considers that, as a default, decisions authorising surveillance should be subject to prior judicial oversight.
- In 2011, we recommended that all interception warrants should be judicially authorised. In June 2015, the Independent Reviewer of Terrorism Legislation agreed. These decisions should no longer be taken by Ministers, but by Judicial Commissioners who hold or who have held "high judicial office" (paragraphs 6 -11).
- The Judicial Commissioners should form part of a new Independent Surveillance and Intelligence Commission ("ISIC") (as recommended by the Independent Reviewer). ISIC should be supported by staff with appropriate technical and cross-disciplinary expertise (paragraph 11).
- JUSTICE recommends that the power of the Secretary of State to certify that a warrant is necessary, subject to judicial supervision, should be strictly limited to cases involving the defence of the United Kingdom or its foreign policy. This certification power should be limited to the interception of communications of a person or persons in a country or territory outside of the UK. A wider "national security" trigger would be overbroad (paragraph 13).
- JUSTICE recommends that requests for access to communications data should also be subject to prior judicial oversight. Responsibility for authorising access should fall to ISIC. A dedicated body of specialist magistrates within ISIC should deal with these decisions, subject to the oversight of the Judicial Commissioners (paragraph 27).
- While the reports of the ISC, the RUSI panel and the Independent Reviewer each suggest distinctions may be possible for some kinds of communications data, none agree on a suitable categorisation. In JUSTICE's 2011 report, it also suggested an exemption for subscriber data sought by police, intelligence and emergency services. However, the default creation of exemptions for data deemed inherently less sensitive than others is questionable. JUSTICE recommends prior judicial authorisation for all requests, subject to an emergency authorisation procedure akin to that already in place under Part 2 of the Regulation of Investigatory Powers Act 2000 (paragraph 27).
- Intrusive surveillance warrants should also be subject to prior judicial authorisation, including those currently authorised by the Secretary of State in respect of the intelligence services (paragraph 28). Similarly, the use of covert human intelligence sources and warrants for encryption keys should be subject to judicial oversight (paragraphs 30 and 35).
- There is a substantial case for further reform of the use of covert human intelligence sources (paragraphs 29 – 30). Any proposals for powers to ban encryption or to allow for easier access to encrypted material should be treated with caution by Parliament (paragraph 35).

The Investigatory Powers Tribunal

- JUSTICE shares the Independent Reviewer's view that recent efforts by the Investigatory Powers Tribunal ("IPT") to increase the transparency of its procedures are welcome. However, both the Independent Reviewer and the RUSI panel recommend that changes are necessary to improve the role of the IPT. JUSTICE reiterates its 2011 recommendations for the improvement of the function of the IPT and the accessibility of its procedures:
    - ISIC Judicial Commissioners should be empowered to refer cases to the IPT.
    - Judicial Commissioners should be under a duty to notify subjects of surveillance after a surveillance operation has ended, to allow them to bring a complaint to the Tribunal in cases where an authority has acted unlawfully. This duty would be subject to a requirement that notification would not compromise any ongoing investigation.
    - The Tribunal should be empowered to undertake proactive investigations or in any case where there are reasonable grounds to suspect unlawful use of surveillance by a public body.
    - The procedures of the IPT should be changed to allow greater transparency and the testing of relevant evidence, including through the appointment of special advocates to represent the interests of an excluded party (paragraph 36).
- We welcome the recommendation of both the RUSI panel and the Independent Reviewer that decisions of the IPT should be subject to appeal (paragraph 41).

Oversight and accountability

- In 2011, we recommended the consolidation of the Chief Surveillance Commissioner's Office, the Intelligence Commissioner's Office and the Interception Commissioner's Office into a single, coherent body with enhanced powers and greater capacity to conduct effective, credible oversight of surveillance decision making.

  JUSTICE supports the creation of a single body with responsibility for authorisation and oversight, following the ISIC model, recommended by the Independent Reviewer, as a *"well-resourced and outward-facing regulator both of all those involved in the exercise of surveillance powers and of the security and intelligence agencies more generally"* (paragraphs 42 – 45).

  We consider that there are likely to be significant benefits from having a pool of judges with expertise in surveillance matters, capable of taking independent and authoritative decisions on authorisation and oversight, supported by an independent body with a high level of technical and cross-disciplinary expertise. These benefits will, of course, be subject to the provision of adequate funding and support (paragraph 47)

Introduction

1. Four years ago, JUSTICE published *Freedom from Suspicion: Surveillance Reform for a Digital Age.*[1] It concluded that the existing UK legal framework governing the use of surveillance powers – most notably the Regulation of Investigatory Powers Act 2000 ('RIPA') – was "*poorly drafted and hopelessly opaque*", "*badly out of date*" and lacking in effective safeguards against abuse.

2. It recommended "*root and branch reform of the law on surveillance*" in order to protect fundamental rights, including:

(i) judicial authorisation of interception warrants;[2]

(ii) judicial authorisation of requests by public bodies for access to communications data;[3]

(iii) greater clarity concerning the statutory definitions of 'intrusive' and 'directed' surveillance;[4]

(iv) judicial authorisation for the use of undercover police officers in complex operations;[5]

(v) stricter controls on the use of encryption key notices;[6]

(vi) improving the fairness of proceedings before the Investigatory Powers Tribunal, including relaxing the policy of 'neither confirm nor deny';[7] and

(vii) rationalising the existing oversight arrangements for investigatory powers into a single oversight body supervising the use of surveillance powers by the police, intelligence services and all other public bodies.[8]

3. Since we first published these recommendations in October 2011, there have been a number of significant developments relating to surveillance and privacy, both in the UK and abroad. In the past year alone, the Investigatory Powers Tribunal has found violations of the right to privacy under Article 8 of the European Convention on Human Rights by the intelligence services on three different occasions; the Divisional Court disapplied section 1 of the Data Retention and Investigatory Powers Act 2014 because it breached the rights to privacy and data protection under the EU Charter of Fundamental Rights; and the Intelligence and Security Committee and the Independent Reviewer of Terrorism Legislation have each produced major reports on the legal framework governing surveillance powers.[9] In June,

---

[1] JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age* (2011) ('*Freedom from Suspicion*').
[2] *Freedom from Suspicion*, paras 141-143.
[3] With the exception of requests for subscriber data by police, other law enforcement agencies, the intelligence services and the emergency services: see *Freedom from Suspicion*, paras 190-193.
[4] Ibid, paras 224 and 283-284.
[5] Ibid, paras 306-307.
[6] Ibid, paras 343-347.
[7] Ibid, paras 395-400.
[8] Ibid, para 407(ii) et al.
[9] In addition, in March 2014 the then deputy prime minister, Nick Clegg MP, asked the Royal United Services Institute to coordinate a

the Home Secretary announced that the government would publish a draft Bill governing the use of investigatory powers in Autumn, for consideration by a pre-legislative committee of both Houses, with the intention of introducing a Bill in Parliament early in 2016.[10]

4. In light of these developments, and with the prospect of fresh legislation to be introduced shortly, JUSTICE has produced this update to our 2011 report in order to inform the forthcoming debate.

5. JUSTICE remains committed to the effective protection of individual privacy in the legal framework for surveillance powers. We hope that all of our recommendations in our 2011 report will inform the new debate on reshaping our standards for a digital age. As an organisation, we focus squarely on the operation of the justice system and in this publication, we focus principally on fair decision making, access to justice and redress in surveillance, and on three priorities: authorisation, the role of the Investigatory Powers Tribunal and oversight and accountability.

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*.

[10] Statement of Theresa May MP, Secretary of State for the Home Department, on the Anderson Report, HC Deb, 11 June 2015, Col 1354.

Authorisation and surveillance

Interception warrants

6. In 2011, we recommended that applications for interception warrants should no longer be made to the Secretary of State but instead made *ex parte* to a security-cleared High Court judge.[11] We also recommended that there should be provision for self-authorisation by the intercepting agency in cases of emergency, subject to judicial confirmation within 48 hours – a practice consistent with judicial authorisations in other common law jurisdictions such as the United States[12] as well as with the emergency use of intrusive surveillance by police under section 36(3) of RIPA.[13]

7. In addition, we proposed that judges should have the power, in sufficiently complex cases, to direct the appointment of a special advocate to represent the interests of any affected person and the public interest in general.[14] For the past 15 years, for instance, it has been a statutory requirement in Queensland to appoint a Public Interest Monitor to supervise all applications for the use of surveillance devices.[15] In October 2011, Victoria also introduced a Public Interest Monitor in respect of applications for interception and surveillance.[16] 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.[17]

8. In its report in March, the ISC recommended retaining the existing system of executive authorisation on the basis that government ministers "*are able to take into account the wider context of each warrant application and the risks involved, whereas judges can only decide whether a warrant application is legally compliant"*.[18] An additional reason given by the ISC was that it was "*ministers, not judges, who should (and do) justify their decisions to the public*".[19]

9. However, the ISC's concern that ministers "*are able to take into account the wider context of each warrant application*", whereas judges are not, is misplaced. There is nothing to prevent the Secretary of State making the initial decision to authorise the interception of communications so long as that decision does not become effective until it is approved by a judge: indeed, this model is already established in the case of TPIMs,[20] deportation on national security grounds,[21] and – indeed – the use of intrusive surveillance by police under section 36 of RIPA. To the extent that the "*wider context*" is relevant, therefore, that is a matter for the Secretary of State to determine at a stage prior to judicial authorisation. It

---

[11] *Freedom from Suspicion*, para 141.
[12] 18 US Code § 2518(7), as provided by Title III of the Omnibus Crime Control and Safe Streets Act 1968.
[13] See *Freedom from Suspicion*, paras 88 and 205.
[14] *Freedom from Suspicion*, para 141.
[15] See Police Powers and Responsibility Act 2000 (Qld) s 740(1) and Crime and Misconduct Act 2001 (Qld) s324(1).
[16] Public Interest Monitor Act 2011 (Vic).
[17] See e.g. "Abbott government and Labor reach deal on metadata retention laws", Sydney Morning Herald, 19 March 2015.
[18] Para 203FF.
[19] Para 203GG.
[20] See s 6 of the Terrorism Prevention and Investigation Measures Act 2011.
[21] See the Special Immigration Appeals Commission Act 1997.

would be improper, however, to suppose that having regard to the "*wider context*" could ever justify a decision that was unlawful.

10. As to the democratic accountability of government ministers, we noted in 2011 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*".[22] 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.

11. In his report published in June 2015, the Independent Reviewer agreed with our 2011 recommendation that interception warrants should be judicially authorised, suggesting that "*the appropriate persons to perform this function would be senior serving or retired judges in their capacity as Judicial Commissioners.*"[23] We agree with this proposal. Although our 2011 report suggested that the appropriate person would be a High Court judge, we consider that any person who either holds or has held "high judicial office" within the meaning of section 60(2)(a) of the Constitutional Reform Act 2005 would be suitable.[24] As we explain further below, we consider that the Judicial Commissioners should form part of the Independent Surveillance and Intelligence Commission (ISIC) proposed in *A Question of Trust*, where ideally they would be supported by staff with the appropriate technical and cross-disciplinary expertise.

12. In the case of warrants involving "*the defence of the UK or its foreign policy"*, the Independent Reviewer recommended that 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 would have the power to depart from that certificate, 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.

13. We note the Independent Reviewer is careful to distinguish the "*defence of the UK or its foreign policy*" from "*national security*" more generally, and states specifically that

---

[22] *Freedom from Suspicion*, para 85.
[23] AQOT, para 14.47.
[24] This is, for example, the requirement for the appointment of the Surveillance Commissioners under s 91 of the Police Act 1997.
[25] Ibid, para 14.64.

the certification procedure would not apply to "*national security warrants of a domestic nature*", including terrorism, which he rightly describes as "*criminal activity*".[26] We would not, therefore, oppose certification if restricted to the grounds of defence and foreign policy. We would propose, however, an additional condition that certification may only be used in relation to a warrant to intercept the communications of a person or persons in a country or territory outside the United Kingdom. We would, in any event, strongly oppose the introduction of certification on the much broader grounds proposed by the RUSI review, namely "*national security (including counter-terrorism, support to military operations, diplomacy and foreign policy) and economic well-being*".[27] As perhaps RUSI did not appreciate, "*national security*" is a term of considerable breadth under UK law and, in many cases, unhelpfully so.[28] As the Reviewer notes, the benefits of judicial authorisation would be reduced "*if the Home Secretary were effectively given the power to decide whether a particular warrant was necessary in the interests of national security*".[29]

14. Our 2011 report was primarily concerned with the operation of surveillance powers within the United Kingdom. It did not, therefore, deal with warrants for the interception of "*external communications*" under section 8(4) RIPA, which do not involve any targeting of specific individuals or premises as is required under section 8(1). This proceeded from our understanding that there was, on its face, very little overlap between the section 8(1) regime governing the interception of communications within the United Kingdom, on the one hand, and the section 8(4) regime relating to overseas communications, on the other. Following the revelations of Edward Snowden in June 2013, however, it has become apparent that this understanding was entirely mistaken. It now appears that section 8(4) warrants have been used to authorise the bulk interception of *all* internet-based communications transiting certain fibre optic cables, including a significant proportion of communications which are properly "*internal*", i.e. those between two persons who are both within the United Kingdom.[30] In May 2014, a witness statement given by a Home Office official confirmed publicly for the first time that internet-based communications such as a Facebook post or a Google search were regarded by the government as "*external*" communications for the purposes of section 20 RIPA even where both the sender and the recipient of the message were within the UK.[31] The March 2015 report of the Intelligence and Security Committee similarly confirmed the potential extent and scope of bulk interception under section 8(4) warrants.[32] As with our 2011 report, this paper does not address the use of bulk interception of communications or the extraterritorial application of surveillance powers in any detail. It is plainly a matter of grave concern, however, that the narrow and targeted requirements of an interception warrant under section 8(1) may be sidestepped by the bulk interception of *exactly the same private communications* under section 8(4). More generally, we question whether the very practice of intercepting potentially millions of private communications without suspicion could ever satisfy the fundamental requirements of proportionality under

---

26 Ibid.
27 See recommendation 10 of the RUSI review.
28 See e.g. *Secretary of State for the Home Department v Rehman* [2001] UKHL 47 per Lord Steyn at para 17; *Miranda v Secretary of State for the Home Department and others* [2014] EWHC 255 (Admin) per Laws LJ at paras 26 and 36.
29 AQOT, para 14.64.
30 See e.g. "GCHQ taps fibre-optic cables for secret access to world's communications", *The Guardian*, 21 June 2013.
31 Witness Statement of Charles Farr, Director General of the Office for Security and Counter-Terrorism, 16 May 2014, paras 126-141.
32 ISC report, pp 25-32.

international human rights law.[33]

Access to communications data

15. Four years ago, we recommended that the requirement for prior judicial approval of requests by local authorities for access to communications data that was subsequently established under section 37 of the Protection of Freedoms Act 2012 should be extended to all other public bodies, except in relation to requests for access to subscriber data by the police, law enforcement, the intelligence services and the emergency services.[34]

16. As we noted at the time, a major problem with requests for communications data was "*the increasingly intrusive nature of the data itself*".[35] It was, therefore, a mistake to assume that access to such data was necessarily less intrusive than interception. On the contrary, we argued that there were "*a number of circumstances*" in which the intrusion could be "*as severe as that posed by interception*".[36]

17. The past four years have seen a growing recognition of the highly sensitive nature of communications data. 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*".[37] 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".*[38]
>
> *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.*[39] *The Court went on to approve Justice Sotomayor's 2012 description of GPS*

---

[33] We also note the ISC's reference at paras 42-45 to so-called 'thematic' warrants where the reference to a specified "person" for a targeted interception warrant under s 8(1) RIPA may include, by virtue of section 81, "any organisation and any association or combination of persons". The ISC report quotes the Home Secretary as saying that "the group of individuals must be sufficiently defined to ensure that I, or another Secretary of State, is reasonably able to foresee the extent of the interference and decide that it is necessary and proportionate". We note, however, that this guidance had never been made public until the ISC published its report and we doubt whether this satisfies the requirements of legal certainty and clarity under Article 8 ECHR in any event.

[34] The reason for treating police, intelligence and the emergency services differently in relation to subscriber data - but not traffic data or service use data - was simply to reflect the fact that subscriber data was primarily useful in identifying a particular individual as opposed to the details of their communications or, indeed, their movements.

[35] *Freedom from Suspicion*, para 182-186. Referring to the decision of the ECtHR in *Malone v United Kingdom* (1984) 7 EHRR 14, for instance, we said "it is clear that access to the location data of a person's phone is likely to disclose far more information concerning their conduct than the now-antiquated meter that the Post Office attached to Mr Malone's phone line in the late 1970s" (para 185).

[36] *Freedom from Suspicion*,, para 190.

[37] 573 US (2014) per Roberts CJ at 9.

[38] 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).

[39] 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*

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".[40]

18. In April 2014, the Grand Chamber of the Court of Justice of the European Union similarly observed that the provisions of the Data Retention Directive applied to "*all means*" of electronic communication, "*the use of which is very widespread and of growing importance in people's everyday lives*".[41] Accordingly, the mandatory retention under the Directive of data relating to those communications entailed "*an interference with the fundamental rights of practically the entire European population*".[42]

19. More anecdotally, Stewart Baker, the former senior counsel to the US National Security Agency told an audience in 2013 that communications data "*absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content*".[43] The former head of the NSA, General Michael Hayden, was even more frank in his comments in April 2014, stating: "*We kill people based on metadata*".[44] In its March 2015 report, the ISC expressed its surprise at learning that "*the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications*".[45]

20. In February 2015, the Interception of Communications Commissioner published the conclusions of his inquiry into the police use of their powers to access communications data under Part 1 of RIPA in order to identify journalistic sources. Among other things, the Commissioner concluded that the current Home Office Code of Practice governing access to communications data did not provide "*adequate safeguards*" to protect journalistic sources or prevent "*unnecessary or disproportionate intrusions*".[46] In addition, he recommended that "*judicial authorisation must be obtained in cases where communications data is sought to determine the source of journalistic information*".[47] In cases where the purpose of the investigation was not to identify a source, it was not necessary to obtain judicial authorisation "*so long as the designated person gives adequate consideration to the necessity, proportionality, collateral intrusion, including the possible unintended consequence of the conduct*".[48] Notably, neither the Commissioner's report nor the now-revised Code of Practice issued in March 2015[49] make any reference to the fact that the obligation to protect journalistic sources under Article 10 ECHR extends to the sources of non-governmental organisations.[50]

---

phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building".

40 565 US (2012) at 3, cited at *Riley*, ibid, at 20.

41 Cases C293/12 and C594/12 Digital Rights Ireland, para 56.

42 Ibid.

43 Alan Rusbridger, "The Snowden Leaks and the Public", *New York Review of Books*, 21 November 2013.

44 David Cole, "We Kill People Based on Metadata", *New York Review of Books*, 10 May 2014.

45 ISC report, para 80.

46 Interception of Communications Commissioners Office, *Inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources* (4 February 2015), paras 8.7-8.10.

47 Ibid, para 8.9.

48 Ibid.

49 Home Office, *Acquisition and Disclosure of Communications Data Code of Practice* (March 2015).

50 See e.g. the judgment of the European Court of Human Rights in *Társaság A Szabadságjogokért v Hungary* (37374/05, 14 April 2009) at para 27: "*The applicant is an association involved in human rights litigation with various objectives, including the protec-*

21. 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*".[51] 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).[52]

22. RUSI likewise distinguished between "*communications data*" and "*content data*",[53] its main recommendations on this point being, first, a review of the existing statutory definitions[54] but also, secondly, judicial authorisation for the acquisition of communications data in bulk.[55] In respect of the acquisition of communications data "*otherwise than in bulk*", RUSI considered that the existing authorisation regime was sufficient.[56]

23. In his report, the Independent Reviewer acknowledged the increased sensitivity of communications data[57] and went on to make a series of detailed recommendations concerning the authorisation process, building on the existing scheme of designated persons (DPs) and single points of contact (SpoCs) which he described as providing "*robust and effective pre-authorisation scrutiny, as well as measure of independence*".[58] He recommended, however, the requirement for judicial approval by a magistrate or sheriff for local authorities should be abandoned[59] on the basis that, "[*w]hilst judicial approval at this level may sound like a safeguard, and was no doubt required for that reason, the reality appears to have been that it has added time, complexity and cost to the authorisation process without contributing additional rigour to it*".[60]

24. In its place, the Independent Reviewer proposes firstly, that where any public authority seeks access to communications data "*for the purpose of determining matters that are privileged or confidential*", it should either be refused by the designated person or referred to the Independent Surveillance and Intelligence Commission (ISIC) "*for determination by a Judicial Commissioner*".[61] In circumstances where data is not sought for such a purpose

---

tion of freedom of information. It may therefore be characterised, like the press, as a social "watchdog" …. the Court is satisfied that its activities warrant similar Convention protection to that afforded to the press." Para 6.31 of the Commissioner's report notes that the term 'journalist' "*for the purposes of this inquiry means any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication".* It goes on to cite the explanation given by Professor Anne Flanagan that it is irrelevant whether *"those that engage in journalism are paid or work for traditional media*". It does not, however, make any reference to the repeated and explicit guidance of the ECtHR on this point.

51 ISC report, para 143(i).

52 Ibid, para 143W.

53 RUSI report, paras 1.40-1.46.

54 Recommendation 3.

55 Recommendation 9(2). Unhelpfully perhaps, the RUSI report did not specify what might constitute 'bulk' access but it appears from the context of its discussion of the issue that it was primarily concerned with where data is gathered under a s 8(4) warrant rather than the powers of Chapter 2 of Part 1 of RIPA.

56 Recommendation 9(3).

57 AQOT, para 14.86 and e.g. the submissions of civil society summarised at para 12.27-12.28.

58 AQOT, para 14.87.

59 AQOT, para 66.

60 AQOT, para 14.82, and see also the criticisms of law enforcement bodies detailed at paras 9.98-9.100.

61 AQOT, para 14.85.

"*but relates to persons who handle privileged or confidential information*" such as doctors, lawyers, journalists and MPs, "*special consideration and arrangements should be in place, and the authorisation should be flagged for the attention of ISIC*". The Reviewer further proposes that, "*where a novel or contentious request for communications data is made, the [designated person] should refer the matter to ISIC for a Judicial Commissioner to decide whether to authorise the request*", with a Code of Practice and/or ISIC providing further guidance on when referrals should be made.[62] These latter recommendations were made "*in recognition of the capacity of modern communications data of a highly personal nature*".[63]

25. However, each of these various recommendations has now been overtaken by the judgment of the Divisional Court in *R(Davies and another) v Secretary of State for the Home Department* in July 2015, in which it disapplied section 1 of the Data Retention and Investigatory Powers Act 2014 on the grounds that it breached the rights to privacy and data protection under the EU Charter of Fundamental Rights.[64] In particular, the Divisional Court held that the existing requirements of Chapter 2 of Part 1 of RIPA were incompatible with EU law because access to retained data was not "*dependent on a prior review by a court or an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued*".[65] The Secretary of State's appeal was heard by the Court of Appeal in late October but, whatever its decision, it seems unlikely that its ruling will be the last word on the matter.

26. In 2011, we recommended prior judicial authorisation for requests to access communications data by *all* public bodies, save in the case of subscriber data which we considered the police, intelligence services and emergency services should be able to access without prior judicial authorisation (but subject nonetheless to the same broad safeguards that are currently applicable). We sought to distinguish subscriber data from other kinds of communications data on the basis that it is primarily used to ascertain a person's identity as opposed to tracking their movements or profiling their behaviour. We took the view that it would be an unnecessary burden on the police or the emergency services, etc, to obtain judicial authorisation simply in order to identify the account holder of a given telephone number or IP address. We also favoured extending the model established by the Protection of Freedoms Act 2012 (which at the time of our recommendation was still before Parliament), involving prior approval by a magistrate.

27. Reviewing the developments since 2011, however, we have had cause to revise our previous recommendations as follows:

a) First, we no longer consider that ordinary magistrates and sheriffs are the appropriate bodies for authorising requests for access to communications data. In this respect, we note the criticism made by the Interception of Communications Commissioner and the evidence recorded in the Independent Reviewer's report.[66] As the Divisional

[62] AQOT, recommendations 70 and 71 and see also para 14.85.
[63] Ibid.
[64] [2015] EHWC 2092 (Admin).
[65] Ibid, paras 91 and 97-98.
[66] AQOT, paras 9.98-9.100.

Court noted in Davies, however, those criticisms were "essentially of lack of training of magistrates, instances of a failure by magistrates to carry out proper scrutiny of applications, failure by the Ministry of Justice to introduce an electronic system to avoid delay and the requirements in some cases for payment of fees".[67] As it went on to note, the need for approval "to be by a judge or official wholly independent of the force or body making the application should not, provided the person responsible is properly trained or experienced, be particularly cumbersome".[68] Instead, in the interests of consistency, responsibility for authorising communications data requests should fall to ISIC, the new oversight body proposed by the Independent Reviewer. Rather than make the Commissioners themselves responsible for authorising requests, however, we recommend the training and appointment of a dedicated body of specialist magistrates within ISIC to deal with such requests. We note that there are already bodies of specialist magistrates within the existing court service: see e.g. those at the City of Westminster Magistrates' Court who deal with requests for extradition, or the magistrates who sit in the Family Proceedings Courts. We consider, therefore, that the most appropriate way forward would be to develop a similar body of specialist magistrates within ISIC itself.

b) Secondly, we no longer consider that it would be appropriate to exempt requests for subscriber data by the police, intelligence services and emergency services from the requirement for prior judicial authorisation. On reflection, it is apparent that it is extremely difficult to draw meaningful distinctions in relation to different types of communications data. In particular, the idea that there are some types of data that are *inherently* less sensitive than others seems to us particularly questionable. Although the reports of the ISC, the RUSI panel and the Independent Reviewer each suggest various distinctions which might support the need for greater safeguards in particular cases, it is telling that there is very little agreement between them as to the precise distinctions to be drawn, and the particular safeguards in each case. In particular, it does not seem satisfactory to leave to designated persons within public bodies the decision of whether a particular request is "*novel*"[69] or "*contentious*"[70] or "*likely to involve collateral intrusion*",[71] etc, particularly while there remains serious doubts as to whether the designated person is sufficiently independent in the first place for the purposes of EU law and the ECHR. In the circumstances, the wiser and most workable course would be to require prior judicial authorisation for *all* requests for communications data, with the only exception being an emergency authorisation procedure along the lines of that already in place under Part 2 of RIPA.[72]

---

67 *Davies and another*, para 97. Emphasis added.
68 Ibid, para 98.
69 AQOT, recommendations 70-71.
70 Ibid.
71 Interception of Communications Commissioners Office, Inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources (4 February 2015), paras 8.9.
72 See section 35(b) which allows authorisations for intrusive surveillance to be made without prior judicial approval on an emergency basis, subject to subsequent review by a judge. As we noted in para 88 of our 2011 report, emergency authorisation procedures of this kind are a common feature of surveillance laws in those jurisdictions which prior judicial authorisation is otherwise a standard requirement.

Intrusive and directed surveillance

28. In 2011, we recommended broadening the definition of 'intrusive' surveillance under Part 2 of RIPA to cover *all* surveillance likely to constitute a serious interference with a person's privacy under Article 8 ECHR, including *any* surveillance of privileged communications, confidential personal information or confidential journalistic information.[73] We further recommended that all warrants for the use of intrusive surveillance (e.g. the planting of listening devices and hidden cameras) should be authorised by a judge, including those currently authorised by the Secretary of State in respect of the intelligence services.[74]

29. The Independent Reviewer did not consider that the use of Part 2 powers fell within the scope of his review of investigatory powers.[75] The ISC did address the use of intrusive and directed surveillance in its report but not in any particular detail nor did it make any significant recommendations in respect of them.[76] The RUSI review also made passing reference to the Part 2 powers, and recommended that there should be "*a periodic review of which public bodies have the authorisation to use intrusive powers*".[77] It is unfortunate, in our view, that the use of intrusive and directed surveillance do not appear to have been the subject of any detailed consideration particularly as, in certain circumstances, their use may prove to be far more intrusive than any interception of private communications or access to communications data.

Covert human intelligence sources

30. Four years ago, we recommended the extension of prior judicial authorisation for the use of covert human intelligence sources to all public bodies, with the exception of the police, the intelligence services and other law enforcement bodies.[78] At the same time, we also recommended that complex operations involving the use of undercover officers should be subject to authorisation by warrant issued by a Surveillance Commissioner.[79] Subsequent revelations concerning the activities of the Special Demonstration Squad, including the apparent exploitation of long-term relationships[80] and infiltration of the Stephen Lawrence Campaign,[81] have only reinforced our view that this is an area in need of substantial reform.

---

[73] *Freedom from Suspicion*, para 244. In relation to 'directed surveillance' we made the corresponding recommendation that its definition should be revised to cover any covert surveillance that seeks to obtain information about an individual but does not otherwise involve significant interference with their privacy, as well as any use of overt surveillance – including CCTV and ANPR – in a targeted manner: see paras 283-284.

[74] Ibid, para 245-246. In relation to directed surveillance, we recommended that there should be prior judicial authorisation for all public bodies except for the police, intelligence services and other law enforcement bodies responsible for investigating and prosecuting serious crime, and for whom the purpose of surveillance is obtaining admissible evidence: paras 285-286.

[75] AQOT, para 6.23.

[76] ISC Report, paras 164-172.

[77] RUSI Report, recommendation 4.

[78] *Freedom From Suspicion*, para 307.

[79] *Freedom From Suspicion*, para 306.

[80] See e.g. "Met police to pay more than £400,000 to victim of undercover officer" by Rob Evans, *The Guardian*, 23 October 2014.

[81] See e.g. "Stephen Lawrence police 'spy' prompts public inquiry", BBC News, 6 March 2014.

Encryption

31. Our 2011 report recommended extending the use of prior judicial authorisation for the use of encryption key notices, including those involving the interception of encrypted communications and the intelligence services.[82] In addition, we recommended that – wherever an encryption notice is sought that would require a person to provide the key to – or otherwise decrypt, his own material, any application should be made *inter partes* to allow him to challenge the proposed notice at the permission stage.[83]

32. In the wake of the revelations by Edward Snowden of extra-judicial hacking by the NSA and GCHQ of various internet service providers, there has been an increasing trend towards the adoption of end-to-end encryption by both service providers and ordinary users alike.[84] Shortly after the attack on the Charlie Hebdo offices in Paris in January 2015, Prime Minister David Cameron stated that he was not prepared to "*allow a means of communication which it simply isn't possible to read*", which was widely interpreted as signalling a move to ban or at least more strictly control the use of encryption.[85] The ISC report similarly asked whether communications service providers should "*be providing an opportunity for terrorists and others who wish to do us harm to communicate without inhibition?*"[86]

33. In his report, however, the Independent Reviewer noted the existence of the forced decryption powers under Part 3 of the Act, which still do not appear to be widely used.[87] He also added that "*neither the [intelligence agencies] nor anyone else has made a case to me for encryption to be placed under effective government control*".[88] The RUSI panel similarly stated that "*we do not believe that the police, law-enforcement agencies and SIAs should have blanket access to all encrypted data, by legally requiring the handover of decryption keys, for example*".[89]

34. In May 2015, the UN Special Rapporteur on Freedom of Expression issued a report on encryption and anonymity.[90] Among his key findings were that "*outright prohibitions on the individual use of encryption technology disproportionately restrict the freedom of expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression, without any particular claim of the use of encryption for unlawful ends*".[91] The Special Rapporteur also noted that the practice of some states in requiring so-called back door access similarly "*threatens the privacy*

---

82 *Freedom from Suspicion*, paras 343-344.
83 *Freedom from Suspicion*, para 345.
84 See e.g. AQOT, para 1.6(d).
85 See e.g. "Spies should be able to monitor all online messaging says David Cameron", *Daily Telegraph*, 12 January 2015.
86 ISC Report, para 4.
87 AQOT, paras 8.30-8.31.
88 AQOT, para 10.20. See also para 13.12: "Few now contend for a master key to all communications held by the state, for a requirement to hold data locally in unencrypted form, or for a guaranteed facility to insert back doors into any telecommunications system. Such tools threaten the integrity of our communications and of the internet itself. Far preferable, on any view, is a law-based system in which encryption keys are handed over (by service providers or by the users themselves) only after properly authorised requests."
89 RUSI Report, para 5.45.
90 A/HRC/29/32, 22 May 2015.
91 Ibid, para 40.

necessary to the unencumbered exercise of the right to freedom of expression".[92] Targeted decryption orders, by contrast, were "*less likely to raise proportionality concerns than key disclosure*".[93] Even so, such orders:

> "*should be based on publicly accessible law, clearly limited in scope, focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight*".[94]

35. It is surprising, in light of the current debate, that so little attention has been paid to the power to issue encryption notices under the existing legislation. While it is certainly true that the poor drafting of Part 3 of RIPA has done little to assist public understanding of that power, it is incumbent upon the government to explain why the existing power is inadequate to address the problem of encrypted communications before proposing any further legislation. As our 2011 report set out at some length, the government repeatedly justified the introduction of the powers under Part 3 by reference to national security concerns whereas in fact the available evidence suggests that Part 3 has been little used for that purpose.[95] Parliament should therefore be wary of similar claims being advanced in future to show that the existing powers are inadequate. On the contrary, greater attention must be paid to ensuring judicial authorisation for the use of encryption notices in every case, in accordance with the principles set out earlier this year by the UN Special Rapporteur.

---

[92] Ibid, para 43.
[93] Ibid, para 45.
[94] Ibid.
[95] *Freedom from Suspicion,* paras 333 - 338.

The Investigatory Powers Tribunal

36. Four years ago, we made a series of recommendations concerning the role of the Investigatory Powers Tribunal:

a) oversight commissioners should have the power to refer cases to the Tribunal for investigation whenever he or she reasonably suspects that a public authority has breached the requirements of RIPA, including the unnecessary and disproportionate use of surveillance powers;[96]

b) the adoption of mandatory notification periods, allowing subjects of surveillance to be notified within a reasonable period of time following the conclusion of a surveillance operation that they have been the target of surveillance. This would enable them to bring a complaint to the Tribunal. It would be subject, of course, to the proviso that the relevant oversight Commissioner would have to be satisfied that notification would not compromise any ongoing investigation;[97]

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;[98]

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;[99] 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), in any case where the Tribunal is satisfied that there is a serious issue to be determined and where the public interest in the fair administration of justice outweighs that in the continuing secrecy of the surveillance operation in question.[100]

37. In the wake of the Snowden disclosures, the IPT received a number of complaints concerning the activities of the intelligence services. In addition, complaints have been

---

[96] *Freedom from Suspcion*, para 397.
[97] *Freedom from Suspcion*para 396.
[98] *Freedom from Suspcion*, para 398.
[99] *Freedom from Suspcion*, para 399.
[100] *Freedom from Suspcion*, 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 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").

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),*[101] 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*,[102] 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)*,[103] the IPT held GCHQ's interception of the private communications of two human rights organisations – the Egyptian Center 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 Center that had been the victim of unlawful interception.

38. 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.

39. In its recent report, the ISC praised the Tribunal as "*an important component of the accountability structure*" but nonetheless recommended the introduction of a domestic right of appeal against its decisions.[104] 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;[105] secondly, that its rulings were frequently "*opaque*";[106] that its reliance on complaints brought by the public "*was not a helpful or just arrangement*";[107] and that its recent confusion between Amnesty International and the Egyptian Center for Personal Rights pointed to the need for "*clear procedural improvements that will need to be implemented*".[108] It also endorsed the need for a domestic right of appeal.[109]

---

[101] [2015] UKIPTrib 13_77-H, 6 February 2015.
[102] [2015] UKIPTrib 13_132-H, 13 March 2015.
[103] [2015] UKIPTrib 13_77-H_2, 22 June 2015.
[104] ISC Report, para 217LL.
[105] RUSI Report, para 4.87.
[106] Ibid, para 4.89.
[107] Ibid, para 4.88.
[108] Ibid, para 4.94.
[109] Ibid, para 4.86.

40. 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*".[110] He nonetheless made several recommendations for improvement, including enabling ISIC to notify a subject of an error (subject to not prejudicing ongoing operations) to enable the person to lodge an application to the Tribunal "*in any case in which in the opinion of ISIC it is possible that the scale or nature of the error might entitle the subject of the error to compensation*".[111] He also supported the introduction of a right of appeal from the Tribunal on points of law only.[112] Notably, the Independent Reviewer declined to make any recommendations concerning the Tribunal's procedures, particularly the need for special advocates since "*it can be argued that the nature of IPT cases reduces the need for an advocate to be able to take instructions on behalf of a claimant*".[113]

41. 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 own procedure rules, as the absence of detail in its recent determinations makes plain. We also welcome the recommendations of the Independent Reviewer and the RUSI review supporting a right of appeal and improved notification. In our view, however, the argument for the adoption of a mandatory notification procedure is stronger yet. As we explained in our 2011 report, this does not mean that every person who has been the subject of surveillance would necessarily be notified. It may be that the majority of people are not notified, in most cases because it would prejudice ongoing operations. A mandatory procedure would, however, promote *consideration* of the need for notification at regular intervals, rather than rely on notification on an *ad hoc* basis. Lastly, we differ from the Independent Reviewer on the need for special advocates before the IPT. 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, took no instructions from the excluded parties.

---

[110] APOT, para 14.102.
[111] APOT, recommendation 99 and para 14.103.
[112] APOT, recommendation 114 and para 14.105.
[113] APOT, para 14.108.

Oversight and accountability

42. One of the key recommendations of our 2011 report 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.[114] 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.[115] In the event that that burden was too great for a single body, we suggested the Information Commissioner could take responsibility for overseeing communication data requests by non-law enforcement bodies such as local authorities, fire and ambulance services.[116]

43. Since our 2011 report, we are pleased to note that there has been a marked improvement in the quality of the annual reports produced by the Interception of Communications Commissioner, as well as the transparency of that body more generally. It is no small accomplishment that a body that, only four years ago, was impossible to contact even by post now has a Twitter account. At the same time, it has since become clear that both the Interception of Communications Commissioner and the Intelligence Services Commissioner do no more than conduct a "dip sample" of interception warrants and authorisations, which means that the majority of warrants made in any given year are not in fact subject to judicial scrutiny.

44. In its recent report, the ISC expressed concern at the "*piecemeal"* development of oversight arrangements as the capabilities of the intelligence agencies have increased, and accepted that there was a need for the Commissioners to receive additional resources in order that they could "*look at a much larger sample of authorisations*".[117] The ISC also considered whether to replace the system of Commissioners with that of Inspectors General, as are used in the US, Australia and elsewhere. It resisted this suggestion, however, on the basis that Inspectors General "*often provide more of an internal audit function, operating within the Agencies themselves*", whereas it was "*important to maintain the external audit function that the Commissioners provide*".[118] For reasons known only to themselves, the possibility

---

[114] *Freedom from Suspicion*, para 395.
[115] *Freedom from Suspicion*, paras 145, 198, 247, 287, 307 and 346.
[116] *Freedom from Suspicion*, para 199.
[117] ISC Report, para 211II and JJ.
[118] Ibid, para 211KK.

of combining oversight functions into a single, *external* body was not considered by the ISC.

45. The Independent Reviewer, by contrast, recommended that the existing oversight commissioners should be replaced by a new Independent Surveillance and Intelligence Commission (ISIC),[119] a "*well-resourced and outward-facing regulator both of all those involved in the exercise of surveillance powers and of the security and intelligence agencies more generally*".[120] ISIC would be responsible both for judicial authorisation of interception warrants and (where appropriate) requests for access to communications data,[121] as well as audit and inspection.[122]

46. The RUSI review also favoured combining the functions of the existing oversight bodies into a National Intelligence and Surveillance Office (NISO), an independent public body which would have four main areas of responsibility: inspection and audit, intelligence oversight, legal advice and public engagement.[123] Unlike ISIC, it would not have responsibility for judicial authorisation but it would provide "*support and assistance*" to the IPT and the Judicial Commissioners.

47. Having considered the various proposals, we consider that the ISIC model advanced by the Independent Reviewer is the one that corresponds most closely to our original recommendations. 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[124] 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.

---

[119] AQOT, recommendation 82.
[120] AQOT, para 14.94.
[121] AQOT, recommendations 84-88.
[122] AQOT, recommendations 89-112.
[123] RUSI Report, recommendations 17-18.
[124] AQOT, para 14.98.

Acknowledgements

JUSTICE would particularly like to thank Eric Metcalfe, of Monckton Chambers, author of both this report and *Freedom from Suspicion: Surveillance Reform for a Digital Age*.

We are grateful to Joseph Rowntree Charitible Trust for their funding of *Freedom from Suspicion: Surveillance Reform for a Digital Age* and their subsequent support of JUSTICE. JUSTICE thanks Trust for London for their financial support for this area of our work.

We appreciate the support of King's College London, who jointly hosted a high-level roundtable to explore the issues raised in this report. Particular thanks are due to Dr Cian Murphy, Dickson Poon School of Law.

This report remains the responsibility of the author, JUSTICE. The report has been produced under the supervision of JUSTICE's Director of Human Rights Policy, Angela Patrick.

JUSTICE

59 Carter Lane, London EC4V 5AQ
tel: 020 7329 5100 fax: 020 7329 5055
email: admin@justice.org.uk
www.justice.org.uk