Investigatory Powers Bill 2016: Parts 3 and 4

Briefing for House of Commons Committee Stage

April 2016

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

JUSTICE is concerned that the Investigatory Powers Bill, like the draft Bill and draft Communications Data Bill before it, includes broad provisions for untargeted and bulk powers of surveillance, with insufficiently robust oversight mechanisms for ensuring that these powers are used lawfully and responsibly.

In this briefing, we highlight a number of specific problems in Parts 3 and 4 of the Bill and propose amendments for consideration in Committee.

These include:

i) Greater involvement for the independent Judicial Commissioners and the Investigatory Powers Commissioner in data retention and in the authorisation of access to communications data;
ii) Improved protections for legal professional privilege, journalistic material and the communications of MPs and Peers;
iii) Limits on the scope of the grounds for which communications data can be accessed and restrictions on the number of bodies which can access this intrusive material; and
iv) New protection for whistle-blowers.

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. Since 2011, JUSTICE has recommended that the Regulation of Investigatory Powers Act 2000 ('RIPA') is repealed and replaced by a modern, comprehensive legal framework for surveillance.[1]

2. This new legislation provides a unique opportunity to restore public faith in UK surveillance practices; and to create a framework which is truly "world-leading". However, JUSTICE regrets that this Bill falls short. We welcome the decision by the Government to avow and specify the powers proposed in the Bill. This is an improvement on the existing approach in RIPA and on the proposal for broad delegated legislation in the Draft Communications Data Bill. However, we regret that the powers proposed in the Bill may be overly broad and the safeguards unduly limited.

3. In its briefing on the Bill, JUSTICE has focused principally on issues of authorisation and the judiciary; oversight and the role of the new Investigatory Powers Commissioner ('IPC') and the Investigatory Powers Tribunal ('IPT'). We have raised some wider concerns about the treatment of privileges, legal professional privilege, in particular, and the treatment of intercept material as evidence in legal proceedings.[2]

4. **In this briefing we propose detailed amendments to Parts 3 and 4.**

   Where we do not specifically address an issue, this should not be taken as support for the proposals in the Bill.

[1] JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age,* Nov 2011. 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.*http://www.justice.org.uk/resources.php/305/freedom-from-suspicion Hererin, '*Freedom from Suspicion*'. JUSTICE, *Freedom from Suspicion: Building a Surveillance Framework for a Digital Age,* Nov 2015. http://2bquk8cdew6192tsu41lay8t.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'.*

[2] Fuller briefing on JUSTICE's position on the Bill can be found here: http://justice.org.uk/investigatory-powers-bill/

B. PROPOSED AMENDMENTS AND BRIEFING

Clause 53: Grounds for access to Communications Data

PROPOSED AMENDMENTS

Clause 53, Page 43, Line 39, leave out 'or of preventing disorder'

Clause 53, Page 43, Line 39, after 'detecting' insert 'serious'

Clause 53, Page 43, Line 40, at end, insert 'which includes to assist in investigations into alleged miscarriages of justice'

Clause 53, Page 43, Line 41, leave out sub-clauses (c)-(f) and (i)-(j)

Clause 78, Page 61, Line 8, leave out 'paragraphs (a) – (j) of'

PURPOSE

5. The Bill provides a range of exceptionally broad grounds for public authorities to access retained communications data. These amendments would restrict the list of grounds to circumstances involving serious offences, national security or risk to life and individual well-being.

BRIEFING

6. 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.

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

8. In *Freedom from Suspicion* (2011), JUSTICE explained our concern about the broad scope of the reasons for which public authorities might seek access to communications data:

"Whether it is proportionate, therefore, to run the risk of invading someone's privacy in the knowledge that they may turn out to be innocent depends on several factors, including the reasonableness of the suspicion but also the seriousness of the offence in question. It is the difference, in other words between breaking down the door to someone's hotel room because you think they are being murdered and breaking down the door to their hotel room because you think they have stolen your toothbrush".[3]

9. The Bill as drafted provides for communications data to be accessed for a wide range of purposes, including the assessment and collection of tax and for minor criminal offences and in connection with "financial stability". JUSTICE regrets that the Joint Committee on the draft Bill recommended that local authorities and trading standards authorities should continue to be able to access information under this part, but we welcome their recommendation that Parliament should re-examine the purposes for which data might be sought.[4] While authorities may find it helpful to have access to this kind of intrusion, it is for Parliament to determine whether it would be lawful, proportionate and necessary. This assessment must include an examination of less intrusive means, of course.

10. Parliamentarians should be robust in their scrutiny of each of the individual purposes identified in the Bill. For example, while JUSTICE accepts that in emergency circumstances, access to communications data may be crucial for the purposes of saving life in imminent danger, the definitions on the face of the Bill are very broad. Clause 53(7)(g) would provide for access in any circumstances which may "mitigate" *any* damage to *any* person's physical or mental health.

[3] *Freedom from Suspicion* (2011), para 179.
[4] *Joint Committee Report,* para 83.

PROPOSED AMENDMENTS

Clause 53, page 42, line 21, leave out sub-clause (ii)

PURPOSE

12. The Bill provides for access to retained data to be used for the purposes of testing equipment and systems. This amendment would delete this broad ground for authorisation.

BRIEFING

13. JUSTICE is concerned about the broad provision in the Bill for the powers therein to be used for testing. Members may wish to ask Ministers to explain why this provision is necessary and proportionate.

Clauses 61 – 66 – Public bodies accessing Communications Data

PROPOSED AMENDMENTS

Clause 61, page 49, line 32, leave out sub-clauses (1) and (2) and insert -

(-) For the purposes of this Part, a relevant public authority is:

- **(a) A police force maintained under section 2 of the Police Act 1996**
- **(b) Metropolitan police force**
- **(c) City of London police force**
- **(d) Police Service of Scotland**
- **(e) Police Service of Northern Ireland**
- **(f) British Transport Police Force**
- **(g) Ministry of Defence Police**
- **(h) Royal Navy Police**
- **(i) Royal Military Police**
- **(j) Royal Air Force Police**
- **(k) Security Service**
- **(l) Secret Intelligence Service**
- **(m) GCHQ**
- **(n) National Crime Agency**
- **(o) Criminal Cases Review Commission**

(-) For the purposes of authorisations sought pursuant to Section 53(7)(g) a relevant public authority also includes -

- **(a) A National Health Service Trust established under section 5 of the National Health Service and Community Care Act 1990 whose functions include the provision of emergency ambulance service**
- **(b) A fire and rescue authority under the Fire and Rescue Services Act 2004**
- **(c) Northern Ireland Ambulance Service Health and Social Care trust**
- **(d) Northern Ireland Fire and Rescue Service Board**
- **(e) Scottish Ambulance Service Board**
- **(f) Welsh Ambulance Services National Health Service Trust**

(-) For the purposes of authorisations sought pursuant to Section 53(7)(h), a relevant public authority also includes –

- **(a) Criminal Cases Review Commission**
- **(b) Scottish Criminal Cases Review Commission**

Clause 64, Page 51, Line 9, leave out clause 64

Clause 65, Page 51, Line 30, leave out clause 65

Clause 66, Page 52, Line 6, leave out clause 66.

PURPOSE

15. Schedule 4 currently provides for a lengthy list of bodies who are able to access retained data, including several Government Departments, for example, the Department of Transport and a range of Regulatory Bodies, including for example the Food Standards Agency and the Gambling Authority. This suggests that access to communications data may be accessed for a range of purposes which may be disproportionate and inconsistent with the guidance offered by the European Court of Human Rights.

16. These amendments would reduce the number and type of public authorities able to seek authorisation to access communications data. They would remove the provisions in the Bill which would permit Local Authorities to access retained communications data.

BRIEFING

17. The case law from both the European Court of Human Rights and the Court of Justice of the European Union in *Digital Rights Ireland*[5] make plain that the number and type of persons able to access surveillance powers will be relevant to the assessment of their proportionality.

[5] See [62].

Clause 62 – Delegated powers to expand the number and type of public bodies with access

PROPOSED AMENDMENT

Clause 62, Page 50, Line 22, leave out Clause 62

PURPOSE

18. The Bill provides that the Secretary of State shall be able to modify the list of public authorities able to seek authorisation to access retained communications data by secondary legislation, subject to an enhanced affirmative procedure. Schedule 4 already provides for an exceptionally broad range of public authorities to have access. This amendment would remove the power to amend the list of authorised bodies.

BRIEFING

19. While JUSTICE welcomes the decision to subject these provisions to an enhanced procedure, in light of the already lengthy list of bodies provided in the Bill, Members may wish to consider whether any further power to expand access through delegated legislation would be appropriate.

Clauses 65 – 71: The Single Point of Contact

PROPOSED AMENDMENTS

Clause 65, Page 51, Line 30, leave out Clause 65

Clause 67, Page 53, Line 8, leave out subclauses (a) and (b) and insert –

(a) is an officer appointed by the Investigatory Powers Commissioner;
(b) works subject to the supervision of the Investigatory Powers Commissioner; and
(c) is responsible for advising –
(i) officers of the relevant public authorities about applying for authorisations; or
(ii) designated senior officers of public authorities about granting authorisations.

Clause 69, Page 54, Line 33, leave out Clause 69

Clause 70, Page 55, Line 39, leave out Clause 70

Clause 71, Page 56, Line 17, leave out Clause 71

PURPOSE

20. The Bill provides that authorisations shall be largely self-approved by officials and officers of public bodies, subject to the advice of a Single Point of Contact ("SPoC") within their organisation responsible for advising on the lawfulness of any authorisation. Local authorities, police forces and public bodies who are too small to have their own SPoC are required by the Bill to enter into collaboration agreements with others.

21. These amendments would amend the Bill to provide for the SPoC scheme to be operated under the authority of the Investigatory Powers Commissioner. JUSTICE believes that the value and credibility of any SPoC model would be enhanced by ensuring its independence from the public authorities seeking to use the intrusive powers in the Bill. This would also remove the need for collaboration agreements as the SPoC advisers would be centralised within the IPC framework. It would encourage standardised approaches to the advice given and consistency in the application of the law.

BRIEFING

22. The provision in the Bill consolidates existing practice on the guidance issued by Single Points of Contact, in the self-authorisation regime. The Joint Committee on the Draft Communications Data Bill recommended consolidation in this manner, under the leadership of police forces.

23. However, while the Single Point of Contact remains embedded within the same organisations who seek to access the intrusive material, they cannot be considered independent for the purposes of the role they play in the authorisation process. While they may add practical assistance to officers and agents, they do not significantly increase public confidence in the process.

24. JUSTICE recommends that the Single Point of Contact framework, if continued, should operate as part of an overriding single oversight body, or under the auspices of the Investigatory Powers Commissioner. This would create a single consistent body of staff capable of providing help, assistance and guidance before the final determination of any application. It would also remove the need for collaboration agreements as proposed in the Bill.

Clauses 67 – 79: Principles and privacy

PROPOSED AMENDMENTS

Clause 67, Page 53, Line 25, leave out ‘,and’

Clause 67, Page 53, Line 27, insert the following new subclauses –

(a) the public interest in the protection of privacy and the integrity of personal data; and
(b) the public interest in the integrity of communications systems and computer networks.

Clause 67, Page 53, Line 37, leave out ‘,and’

Clause 67, Page 53, Line 38, insert the following new subclauses –

(a) the public interest in the protection of privacy and the integrity of personal data; and
(b) the public interest in the integrity of communications systems and computer networks.

Clause 79, Page 62, Line 34, insert the following new subclauses –

(a) the public interest in the protection of privacy and the integrity of personal data; and
(b) the public interest in the integrity of communications systems and computer networks.

PURPOSE

25. Throughout this part of the Bill public authorities and other decision makers are placed under a duty to consider a range of factors connected to the decision to access retained communications data. These factors include cost and other resource implications and ‘the issues as to the lawfulness of any authorisation’.

26. These amendments would include a specific duty to consider the public interest in the protection of individual privacy and the security of communications systems and computer networks.

BRIEFING

27. Both the Independent Reviewer in *A Question of Trust* and the Intelligence and Security Committee in its Report on the Draft Bill emphasised the importance for privacy principles, and the legality of the use of surveillance powers to be clear in the new legislation.

28. While JUSTICE has focused on a series of specific amendments to increase safeguards for individual privacy, we are concerned that throughout the Bill there appear to be statutory duties on public agencies, officials and agents, and on the Judicial Commissioners to consider factors relevant to national security and the prevention and detection of crime and to the effectiveness of powers or resources expended, but no specific treatment of privacy standards and the public interest. While the Clauses which these amendments attach to do refer to "any issues as to the lawfulness" of the powers, the vagueness of this instruction appears contradictory. Surely the first consideration for any individual considering the exercise of powers under the Act will be its legality? Listing this as a final in the list of a list of other factors to be "considered" seems entirely inappropriate.

29. Members may wish to ask Ministers for a fuller explanation of the statutory duties on the face of the Bill and the objectives of including the factors as provided in the manner in which they are drafted.

Clause 68 – Judicial authorisation and special protections

PROPOSED AMENDMENTS

Clause 68, Page 54, Line 1, leave out 'to identify or confirm journalistic sources'

Clause 68, Page 54, Line 5, leave out from 'for' to 'and' on Line 7 and insert 'further to this Part'

Clause 68, Page 54, Line 18, leave out 'considers' and insert 'determines'

Clause 68, Page 54, Line 19 leave out subclauses (a) and (b) and insert –

(-) that the conduct permitted by the authorisation is necessary for one or more of the purposes in Section 53(7); and

(-) that the conduct permitted by the authorisation is proportionate to what is sought to be achieved by that conduct.

Clause 68, Page 54, Line 29, leave out subsection (7) and insert the following new subclauses –

(-) The Investigatory Powers Commissioner may for the purposes of approving authorisations under this Section appoint Deputy Judicial Commissioners.

(-) A 'Deputy Judicial Commissioner' must be –

(a) in relation to England and Wales, a justice of the peace

(b) in relation to Scotland, a sheriff, and

(c) in relation to Northern Ireland, a district judge (magistrates' courts) in Northern Ireland.

(-) An authorisation under this Section may not grant authorisation in relation to the obtaining by a relevant public authority of communications data —

(a) insofar as the communication consists of matters subject to legal privilege; or

(b) related communications data, insofar as the data relate to the communication of matters subject to legal privilege.

(-) For the purposes of subsection (1), legal privilege means –

(a) Communications between a professional legal adviser and his client or any person representing his client made in connection with the giving of legal advice to the client;

(b) Communications between a professional legal adviser and his client or any person representing his client and any other person with or in contemplation of legal proceedings or for the purposes of such proceedings;

(c) Items enclosed with or referred to in such communications and made:

i. In connection with the giving of legal advice or

ii. In connection with the contemplation of legal proceedings or for the purposes of such proceedings.

(d) Communications made with the intention of furthering a criminal purpose are not subject to legal privilege.

(-) An application which contains a statement that the purpose of an authorisation is to access communications data in connection with communications made for the purpose of furthering a criminal purpose, but which would otherwise attract legal privilege must be considered by a Judicial Commissioner.

(-) A Judicial Commissioner may issue an authorisation sought under subsection (3), if satisfied that:

(a) There are reasonable grounds to believe that the communications data relates to communications made with the intent of furthering a criminal purpose;

(b) That the data is likely to be of substantial value to the investigation in connection with which the application is made; and

(c) That the data concerned is likely to be relevant evidence;

(d) Other proportionate methods of obtaining the data have been tried without success or were not tried because they were bound to fail

(e) It is in the public interest that the authorisation is granted, having regard to the

i. The benefit likely to accrue to the investigation and prosecution if the data is accessed

ii. The importance of the prosecution

iii. The importance of maintaining public confidence in the confidentiality of material subject to legal professional privilege,

(-) A code of practice issued under Schedule 6 must contain provision about—

(a) the steps to be taken to minimise the risk of conduct undertaken pursuant to an authorisation to which this section applies resulting in accidental acquisition of a communication, or communications data, falling within subsection (1);

(b) the steps to be taken if it appears that such conduct has accidentally resulted in acquisition of such a communication or data.'

(-) Where an authorisation issued under this Part would seek to authorise any activity which may involve access to special procedure material, the following subclauses apply.

(-) Special procedure material subject to this Section will include:

(a) Journalistic material other than material which a person holds in confidence

(b) Communications sent by, or intended for, a member of the relevant legislature.

(-) The special procedure authorisation may only be granted on application to a Judicial Commissioner.

(-) The Judicial Commissioner must be satisfied that there are reasonable grounds to believe that:

(a) A criminal offence has been committed

(b) The material is likely to be of substantial value to the investigation of that offence

(c) Other proportionate methods of obtaining the information have been tried without success or were not tried because they were bound to fail

(d) It is in the public interest that the warrant is granted, having regard to the

i. The benefit likely to accrue to the investigation and prosecution if the information is accessed

ii. The importance of the prosecution

iii. The importance of maintaining public confidence in the integrity of journalists' work product, and/or communications with members of relevant legislatures

iv. The public interest in the freedom of expression enjoyed by journalists and the members of the relevant legislatures, including as protected by Article 10 ECHR.

(-) Where data could reasonably be obtained by means of a search and seizure order pursuant to the Police and Criminal Evidence Act 1984, a warrant under this Part will not be in the public interest.

(-) An application for an authorisation concerning journalistic material held in confidence or information for the purpose of identifying or confirming a source of journalistic information, may only be considered by the Investigatory Powers Commissioner, who must be satisfied that there are reasonable grounds to believe –

(a) A criminal offence has been committed

(b) The communications data is likely to be of substantial value to the investigation of that offence

(c) Other proportionate methods of obtaining the information have been tried without success or were not tried because they were bound to fail

(d) It is in the public interest that the authorisation is granted, having regard to the

(i) The benefit likely to accrue to the investigation and prosecution if the information is accessed;

(ii) The importance of the prosecution;

(iii) The importance of maintaining public confidence in the integrity of journalists' work product;

(iv) The public interest in the freedom of expression enjoyed by journalists and the members of the relevant legislatures, including as protected by Article 10 ECHR.

(-) In considering an authorisation concerning journalistic material held in confidence, the Investigatory Powers Commissioner must give notice to the journalist concerned, unless it would not be in the public interest to do so.

(-) If an authorisation is considered without notice, the Investigatory Powers Commissioner must appoint a Special Advocate to represent the interests of the journalist and the person to whom confidence is owed, and the wider public interest in the integrity of journalists sources and freedom of expression, including as protected by Article 10 ECHR.

(-) Journalistic material is held in confidence for the purposes of this section if –

(a) It is held subject to such an undertaking, restriction or obligation;

(b) It has been continuously held (by one or more persons) subject to such an undertaking, restriction or obligation since it was first acquired or created for the purposes of journalism.

PURPOSE

30. The Bill currently provides for authorisations for access to communications data to be authorised by officials and officers in public authorities except in connection with applications by Local Authorities and where the data sought relates to the identification of a journalistic source.

31. These amendments would require all authorisations to be subject to approval by a Judicial Commissioner except in cases where there is an imminent threat to life. They propose special procedures for communications data subject to legal professional privilege and for the protection of journalistic material and the communications data of politicians (modelled on earlier proposals to amend the warrantry for intercept).

32. The amendments also provide for the Investigatory Powers Commissioner to appoint Deputy Judicial Commissioners to consider applications for the authorisation of access to Communications Data. This proposal is made to reflect the significant number of authorisations for access historically made (over 500,000 a year). It provides that Deputy Judicial Commissioners should be magistrates or sheriffs, with a lower level of judicial expertise than a Judicial Commissioner (High Court Judge). Special procedure

material must be authorised by a Judicial Commissioner or the Investigatory Powers Commissioner, to reflect the seriousness of the interference with this kind of material.

33. JUSTICE also supports, in the alternative, amendments prepared by Liberty for this purpose, which would remove the power to make authorisations and notices from the Bill and replace these provisions with a warranting scheme for both access and retention.

BRIEFING

34. Only a very small number surveillance decisions in the Bill will benefit from any judicial involvement. The Interception of Communications Commissioner's Office has stressed that Judicial Commissioners will only be performing a "*very narrow*" part of the oversight envisaged by the Government.[6]

35. Access to communications data, will generally be by someone within the same organisation as the person seeking permission or by the Secretary of State, subject to the involvement of a SPoC. There is provision for Local Authorities seeking access to be subject to warrant from a magistrate, reflecting changes in the Protection of Freedoms Bill 2012.[7]

36. 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 Bill may be out of step with evolving 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).[8] This is likely to inform the consideration by national courts of necessary safeguards and by other international forums, including at the European Court of Human Rights. This decision is being considered afresh in connection with the challenge by Tom Watson MP and David Davis MP to the existing retention model in the Data Retention and Investigatory Powers Act 2014 at the CJEU. This litigation is being heard on 12 April 2016 and a judgment is expected before this Bill passes.

[6] Interception of Communications Commissioner's Office, written evidence, para 8.
[7] Investigatory Powers Bill, Clause 78.
[8] *Digital Rights Ireland*, C-293/12 and C-594/12 8, April 2014.

b. 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.[9]

c. 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*.[10]

37. Members may wish to ask Ministers for a full explanation of their view that the approach in the Bill is consistent with the international standards which bind the UK.

38. JUSTICE considers that specific protection is required for data subject to legal professional privilege and for data generated in connection with the communications of journalists and politicians. The integrity of these particularly important forms of communication are protected by both Article 6 ECHR and Article 10 ECHR respectively.

39. While the Bill proposes some protection for legal professional privilege and for journalistic information, its protection is limited. While authorisation pursuant to Clause 68 provides for authorisations which target journalists sources to be subject to judicial review by a Judicial Commissioner, the review provided for is very limited and does not expressly provide for the judge to consider the public interest, or the necessity and proportionality of authorisation. The Commissioner is tasked primarily with the

[9] *S & Marper v UK*, App No 30562/04, 4 December 2008.
[10] *Roman Zakharov v Russia (*Application no. 47143/06), 4 December 2015 para 260.

consideration of whether grounds – at the time of authorisation – existed which would permit it to be granted.

40. JUSTICE would support a variation to these amendments, in keeping with our earlier proposed amendments, to provide for a certification role for the Secretary of State in cases involving some national security threats, involving defence and foreign policy decisions.

Clause 73: Whistleblowing and the Public Interest

PROPOSED AMENDMENTS

Clause 73, Page 58, Line 34, insert the following new subclause –

(-) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the disclosure was in the public interest

PURPOSE

41. This amendment would create a public interest defence to any offence of unauthorised disclosure. JUSTICE is concerned that, as drafted, it is unclear whether whistleblowers will be adequately protected in making disclosures in the public interest, including to the Investigatory Powers Commissioner and the Judicial Commissioners.

BRIEFING

42. JUSTICE is concerned that provisions in the Bill may risk inadvertently discouraging or preventing individuals within public authorities or agencies or in Communication Service Providers from approaching the Investigatory Powers Commissioner with concerns or communicating with the Commission frankly.[11] Most worryingly, as has been highlighted by Public Concern at Work (PCaW), channels through which intelligence services personnel could report misconduct were uncertain in the Bill.[12]

43. As PCaW has explained, clarity in this area is particularly important in light of the limitations of the protection offered by the Public Interest Disclosure Act 1998 (PIDA). PIDA protects internal disclosure (i.e. to the employer), disclosures to prescribed bodies (i.e. regulatory bodies including MPs) and wider disclosures to bodies and organisations not prescribed (i.e. media outlets), applying different safeguards in connection with each type of disclosure.

[11] Although Clause 43 in the Bill 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. In light of the history of significant misunderstandings and disagreements about the scope of surveillance law, JUSTICE feels it would be regrettable if individuals and organisations were prevented from consulting with the Investigatory Powers Commissioner about good practice and areas of conflict in the application of the law by overly rigid non-disclosure requirements.

[12] Joint Committee, Report on the Draft Investigatory Powers Bill, para 153.

44. There are two exceptions that are relevant to the Bill. Firstly, members of the intelligence service (and member of the armed services) are completely excluded from PIDA's protection, and secondly PIDA protection does not extend to workers in other sectors where their disclosure would breach the Official Secrets Act 1989 (OSA).

45. JUSTICE strongly supports recommendations made by the Joint Committee that the Bill should be amended both so that it specifies that any disclosure to the Investigatory Powers Commissioner 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, and not subject to any criminal penalty. The Joint Committee has made recommendations that provisions should be inserted into the Bill to allow for direct contact to be made between Judicial Commissioners and both Communication Service Providers[13] and security and intelligence agencies.

46. It is unclear whether persons disclosing such information might be liable for other offences. It is far from clear whether similar safe-routes would apply to whistle-blowers disclosing other information pursuant to powers and duties exercised under other parts of this Act, or otherwise subject to the supervision of the IPC. JUSTICE welcomes that Clause 203 makes provision for any disclosure to the IPC "for the purposes of any function of the Commissioner" will be protected in respect of any duty of confidence or any other bar on disclosure. It is unclear whether these measures will cover unsolicited disclosures or only those sought proactively by Commissioners.

47. JUSTICE considers that a safe-route to the IPC will be crucially important in determining its credibility and effectiveness. Members may wish to ask the Minister to provide a further explanation for the intended effects of the Bill and the protection offered to ensure that individual officials and employees of CSPs might seek effective guidance, or may be protected as a whistle-blower if choosing to report unlawful conduct.

[13] Joint Committee, Report on the Draft Investigatory Powers Bill, para 629.

Clause 78 – Judicial Authorisation and Retention Notices

PROPOSED AMENDMENTS

Clause 78, Page 61, Line 36, insert 'and' and the following new subclauses –

(-) only when approved by the Investigatory Powers Commissioner

(-) In deciding whether to approve a notice, the Investigatory Powers Commissioner must determine whether a notice is –

(a) that the conduct required by the notice is necessary for one or more of the purposes in Section 53(7); and

(b) that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct.

Clause 78, Page 61, Line 38, leave out Secretary of State and insert 'Investigatory Powers Commissioner'

PURPOSE

48. The Bill provides for the Secretary of State to impose data retention notices on individual telecommunications operators. These amendments would require individual notices to be approved by the Investigatory Powers Commissioner.

BRIEFING

49. In these amendments, JUSTICE provides for notices requiring the retention of data should be approved by the Investigatory Powers Commissioner. JUSTICE understands that under the Regulation of Investigatory Powers Act 2000, the number of these notices has been relatively small, but their impact may be wide-ranging and can provide for the retention of data about a large number of persons. In light of this significant and broad based impact, Members may wish to consider whether the Investigatory Powers Commissioner should have a primary role in considering their necessity and proportionality.

50. JUSTICE also supports, in the alternative, amendments prepared by Liberty for this purpose, which would remove the power to make authorisations and notices from the Bill and replace these provisions with a warranting scheme for both access and retention.

51. We support the proposal made by Liberty that retention notices should be limited in a manner consistent with the guidance in *Digital Rights Ireland* to provide for greater targeting and specification in the retention framework.

Clause 83 – Modification and variation

PROPOSED AMENDMENTS

Clause 83, Page 64, Line 21, insert at end 'and' and the following new subclause

(-) the variation has been approved by the Investigatory Powers Commissioner

PURPOSE

52. The Bill currently provides for the Secretary of State to make variations to notices to retain data. This amendment would require variations to be approved by the Investigatory Powers Commissioner, consistent with the amendments proposed, above.

BRIEFING

53. JUSTICE is concerned that despite the limited processes for structured authorisation and notification in respect of the retention of data in the Bill, the Bill as drafted provides for a significant power on the part of the Secretary of State to depart from those structures in later varying the scope of notices.

54. Members may wish to ask Ministers to better explain why such a statutory power of variation should lie with the Secretary of State and not the Investigatory Powers Commissioner. This may provide greater reassurance to Telecommunications providers that the scope of notices are not only lawful, necessary and proportionate, but stable and legally certain.

Clause 80: Review of notices for retention

PROPOSED AMENDMENTS

Clause 80, Page 62, Line 37, leave out 'Secretary of State' and insert 'Investigatory Powers Commissioner'

Clause 80, Page 62, Line 40, leave out 'back to the Secretary of State' and insert 'to the Investigatory Powers Commissioner for review'

Clause 80, Page 63, Line 7, leave out 'Secretary of State' and insert 'the Investigatory Powers Commissioner'

Clause 80, Page 63, Line 10 'Secretary of State' and insert 'the Investigatory Powers Commissioner'

Clause 80, Page 63, Line 12, delete subclause (b)

Clause 80, Page 63, Line 25, leave out 'Secretary of State' and 'and the Commissioner'

Clause 80, Page 63, Line 31, leave out 'Secretary of State' and insert 'Investigatory Powers Commissioner'

PURPOSE

55. The Bill currently provides that telecommunications companies may ask the Secretary of State to review the contents of a notice to retain communications data. These amendments would provide for a review instead by the Investigatory Powers Commissioner.

BRIEFING

56. Members may wish to ask Ministers to better explain why such a statutory power of review should lie with the Secretary of State and not the Investigatory Powers Commissioner. The provision of a route of review to the independent oversight body may provide greater reassurance to Telecommunications providers that the scope of notices are not only lawful, necessary and proportionate, but stable and legally certain.

Clause 84: Discretionary disclosure

PROPOSED AMENDMENTS

Clause 84, Page 65, Line 20, after person insert 'except the Investigatory Powers Commissioner or a Judicial Commissioner'

Clause 84, Page 65, Line 26, leave out 'Secretary of State' and insert 'Investigatory Powers Commissioner'

PURPOSE

57. The Bill provides that the contents of any notice which places a requirement or a restriction on a telecommunications operator must not be disclosed for any reason. However, it gives the Secretary of State a discretion to permit disclosure in undefined circumstances.

58. These amendments would make clear that the contents of any notice may be revealed to the Investigatory Powers Commissioner or the Judicial Commissioners. They would transfer responsibility for decisions on disclosure from the Secretary of State to the Investigatory Powers Commissioner.

BRIEFING

59. This is the final in a series of amendments by JUSTICE which propose that – as the single independent oversight body – the office of the Investigatory Powers Commissioner should be granted primary responsibility for the oversight of both data retention and access to communications data.

60. If the determination on the scope of disclosure about notices remains in the discretion of the Secretary of State, there is a question about whether and how disclosure may be controlled by Ministers in practice.

JUSTICE
April 2016