



# Evidence for the Joint Committee for the Investigatory Powers Bill

**21 December 2015**

### **Summary of Points for the Committee to Consider**

- We have concerns with the aggressive timeline for the Investigatory Powers Bill (hereafter the "IP Bill"). There should be a review provision included in the IP Bill to enable the legislation to be re-visited regularly by the Government and revisions to take place in light of experience, especially given the fact that communications technology is ever changing.
- The oversight provisions in Part 8 of the IP Bill require significant enhancement in order to prescribe properly the legal mandate and functions of the "world-leading oversight body" which the Government is seeking to create. 3 of the 6 elements of our oversight wish-list have been partly addressed and the remaining 3 have not been addressed by the clauses. This section of our evidence submission provides a number of key recommendations.
- Clause 171 is a paradox which requires substantial re-drafting and clarification to ensure that a) the delineation of responsibility between the Investigatory Powers Commissioner and the Investigatory Powers Tribunal (hereafter "the IPT") is clear and, b) individuals are able to seek effective remedy.
- Clause 8 (offence of unlawfully obtaining communications data) could have the unintended consequence of undermining the open and co-operative self-reporting of errors and contraventions currently undertaken. There is a real danger that this provision will reduce accountability and individuals' and public authorities' co-operation with our investigations into errors and contraventions.
- Is it desirable to have the same body responsible for authorising investigatory powers and undertaking the post facto oversight of the exercise of those powers? If so, the judicial authorisation and oversight elements of that body must be operationally distinct.
- There appear to be a number of clauses which provide exceptions for national security or which exempt the intelligence agencies from key safeguards (e.g. clauses 47(2), 47(3), 60(2), 60(3) and 61). Are these exceptions, especially the combined effect, justified?
- The Government has not taken the opportunity to bring all of the investigatory powers used by public authorities into the IP Bill. The result is a lack of clarity and inconsistency in application and approval procedures.
- The IP Bill also curiously prescribes different authorisation and modification procedures for targeted equipment interference warrants made on behalf of the intelligence services (or Chief of Defence intelligence) to those made on behalf of law enforcement. The different procedures are confusing and it is not clear on what basis they are justified.

## **Background**

1. Thank you for inviting the Rt Hon. Sir Stanley Burnton, Interception of Communications Commissioner and Joanna Cavan, Head of IOCCO to give oral evidence to the Committee on 2<sup>nd</sup> December 2015. That session focused mainly on the proposals for Judicial Commissioners in the IP Bill.

2. At the request of the Committee we are providing follow up evidence concerning our “oversight wish-list”, published on 2<sup>nd</sup> November 2015. In addition we thought it might be helpful to highlight to the Committee a number of other matters we think important which have not so far been debated in detail during the evidence sessions.

## **Investigatory Powers Bill Timeline**

3. An incredible amount of work has been undertaken by the Government to get the IP Bill to this stage. The IP Bill is a complicated and very significant piece of legislation. A number of the investigatory powers provided for in the IP Bill have been exercised in the past with little or no transparency under vague statutory frameworks and as such they have never before been debated publicly. We welcome the Government's efforts to put these powers on a clearer statutory footing. However, we do have concerns about the aggressive timeline for the IP Bill to be debated and scrutinised.

4. It is important for the public to understand fully the privacy implications of this legislation which enables highly intrusive conduct to be undertaken. The public authorities and those impacted by the conduct will have to live with the operational consequences of this legislation for some time to come. Therefore the detail has to be right. We need to ensure that the legislation satisfies the rule of law, provides enhanced safeguards to increase accountability and transparency and provides the public authorities with the powers they need to counter threats to our national security, to prevent and detect crime and ultimately to protect the public.

5. Unfortunately time has not allowed for us to examine in detail all of the clauses and their likely consequences in this extensive piece of legislation or to submit detailed written evidence to the Committee. We are aware that a number of other key stakeholders have made the same point. As a result we have tried in this submission to concentrate on matters which have not yet been raised or debated publicly by others. A number of witnesses to the Committee have suggested that there should be a review provision included in the IP Bill to ensure that the legislation is re-visited regularly. This is a sensible proposition, first due to the short timeline provided for scrutiny and secondly due to the fact that communications technology is ever changing. We anticipate the need to regularly revise the legislation in light of experiencing new technologies, the trends in uptake and use.

6. To save repetition we would like to signpost the Committee to the issues highlighted in our detailed written evidence<sup>1</sup> to David Anderson QC's Investigatory Powers Review. Our evidence addressed the effectiveness of the current statutory oversight arrangements, the safeguards to protect privacy, the case for amending or replacing legislation and the statistical and transparency requirements that should apply. Many of the issues highlighted were addressed in the Review's report (A Question of Trust) and consequently have flowed into the IP Bill clauses.

7. We also recognise that a number of other experts and key stakeholders have raised concerns (and submitted written evidence) to the Committee on, for example, the clauses relating to thematic interception warrants, modifications to thematic warrants, and the principle of judicial review. We do not seek to repeat those points in our submission, but deem those concerns worthy of serious consideration by the Committee. We also make the point that we are not best placed to comment on the clauses that cover areas outside of our current oversight remit (e.g. bulk personal datasets, equipment interference etc) and we hope that the other Commissioner bodies that oversee those areas will submit evidence on the legitimacy and adequacy of those powers and safeguards.

#### **Oversight wish-list**

8. On 2<sup>nd</sup> November 2015 we published a wish-list containing 6 elements that we thought the IP Bill must contain in order to modernise and strengthen the current oversight of surveillance powers. The elements in our wish-list are set out below along with commentary on whether the IP Bill addresses sufficiently each element. In summary 3 of the elements of our wish-list have been partly addressed and the remaining 3 have not been addressed.

- a. A single independent public facing oversight body – We support fully a single unified body with responsibilities for surveillance oversight. This will present an opportunity to streamline the oversight landscape, to put all of the oversight responsibilities on a statutory footing, to bridge some of the identified gaps and address the overlaps. The body must be independent, have an appropriate legal mandate and be public facing to promote greater public confidence.

Partly addressed – We welcome the creation of a single Investigatory Powers Commission to replace the three current RIPA Commissioner bodies. However the oversight clauses in Part 8 of the IP Bill require substantial re-drafting in order to deliver what the Home Secretary has described as “world leading oversight”. In particular -

---

<sup>1</sup> [http://www.iocco-uk.info/docs/2014-12-5\(2\)%20IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf](http://www.iocco-uk.info/docs/2014-12-5(2)%20IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf)

- **Investigatory Powers Commission** (absent from clauses) - There is no mention of the “Commission” in the IP Bill. The clauses are only concerned with the creation of the Investigatory Powers Commissioner and the Judicial Commissioners (hereafter the “Judicial Commissioners”). There is no clear legal mandate for the oversight body and the clauses do not reflect the breadth of skills required to complement the Judicial Commissioners and ensure the oversight is effective. The reality is that the Judicial Commissioners will only be performing a very narrow part of the oversight – the prior authorisation of some of the more intrusive investigatory powers. The bulk of the oversight will actually be carried out by inspectors and staff within the Commission who need a clear legal mandate to require information from public authorities, to launch and undertake audits, inspections, inquiries, investigations and react in real time when non-compliance or contraventions of the legislation are discovered during an inspection. There are examples of oversight bodies created as separate “Commissions”, e.g. section 9 of the Police Reform Act 2002 created the Independent Police Complaints Commission as a body corporate. We believe this legal structure provides an appropriate model for the Investigatory Powers Commission, with statutory functions vested in the body corporate as well as the Judicial Commissioners.
- **Appointment of Commissioners** (clauses 167 & 168) – It is inappropriate for the Judicial Commissioners to be appointed by the Prime Minister as this dilutes public confidence and independence. The more modern arrangement and increasing standard internationally is for judicial appointments to be made by an independent body rather than the executive. It would be more appropriate for the Judicial Commissioners to be appointed by the Judicial Appointments Commission in consultation with the Lord Chief Justice. In a similar vein Judicial Commissioners should not be removed from office without the agreement of the Lord Chief Justice.
- **Funding, Staff and Facilities** (clause 176) - It is inappropriate for the Secretary of State to be responsible for determining what staff, accommodation, equipment and other facilities are necessary for the carrying out of the Judicial Commissioners’ functions, particularly because those Commissioners will be reviewing the Secretary of State’s authorisations. Again, the more modern arrangement and increasing standard internationally is for the judiciary to determine the resources (including personnel) they require, rather than the executive, and to determine their budget in consultation with the Treasury.
- **Main oversight functions** (clause 169(4)) – A number of witnesses in the oral evidence sessions have stated that it would be preferable and simpler for the Investigatory Powers Commission to also oversee the arrangements within

Communication Service Providers (CSPs) and public authorities for the retention, storage and destruction of communications data. These matters are currently reviewed by the Information Commissioner's Office (ICO), but in the case of public authorities no audits are undertaken by the ICO. We are responsible for overseeing those arrangements where they concern interception. There are further unhelpful consequences of the overlaps at present between IOCCO's oversight of CSP errors under RIPA and the ICO's oversight of breaches under the Privacy and Electronic Communications Regulations (PECR) (where the breaches also constitute RIPA errors). In our view there is still considerable room to revise the oversight provisions to simplify the oversight landscape, avoid overlaps and ensure consistency of decision making.

- **Additional Functions Under This Act** (clause 172(2)) – It would be sensible to include an explicit provision for CSPs and staff within public authorities to refer directly to the Investigatory Powers Commission any complaint or concern they have with conduct proposed or undertaken, or any matter on which they require clarification.
- b. Full access to technical systems – The current statute (RIPA) contains outdated language (a requirement to provide to the Commissioner with “all such documents and information”) and is in need of updating. The query based searches we have developed on the communications data side of our business enable us to identify at scale trends, patterns and compliance issues across large volumes of applications. We need to develop our technical audits on the interception side of the business, particularly where the collection of material and data is at scale.

Not addressed – The IP Bill must contain provision for the “Commission” to be provided with access to technical systems to assist audits, inspections and inquiries to be carried out. Any new technical systems (e.g. secure automated CSP disclosure systems, the request filter, workflow systems managing applications and authorisations) must be developed with oversight and audit functions in mind.

- c. Provision to launch inquiries & investigations and sufficient resource to conduct thematic inquiries – The oversight body should have a clear mandate to launch inquiries into matters of public interest or areas of concern. Detailed thematic investigations should take place in addition to ongoing reviews. It is difficult presently for us to produce detailed thematic reports without undermining our core review functions - both are key elements to ensuring robust oversight and one should not compromise the other.

Not addressed - Clause 169(1) provides that *“the Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of...”* The insertions in brackets appear to be an afterthought and are insufficient. The IP Bill provisions do not compare favourably with the clear powers and legal mandate in place for some of our international counterparts. For example, the oversight provisions for the New Zealand Inspector-General of Intelligence and Security as set out in the Inspector-General of Intelligence and Security Act 1996 (amended in 2013)<sup>2</sup>. The IP Bill oversight clauses could be strengthened significantly in this respect.

- d. Relaxation on secrecy provisions to aid transparency – We are constrained by the current statutory provisions in section 19 of RIPA forbidding disclosure (as are the public authorities and the CSP's). The culture of what appears to be secrecy by default must continue to be challenged and transparency should be encouraged where it leads to greater accountability without prejudicing national security or the ongoing prevention or detection of serious crime.

Partly addressed – Clauses 43 and 44 provide secrecy provisions for interception-related conduct and create an offence of making unauthorised disclosures (similar to the current section 19 RIPA provisions). The Committee may want to consider whether these provisions are necessary. The provision for “authorised disclosures” in clause 43(5) is however a welcome addition and may lead to greater transparency.

- e. Full provision for reporting of errors / breaches and a power to refer to the Investigatory Powers Tribunal (IPT) – It is crucial to ensure that the error reporting provisions are clear and comprehensible and that individuals adversely affected are able to seek effective remedy. On the latter point a number of areas would benefit from review here including; the very high threshold of “wilful or reckless”, whether the Commissioner should be able to refer matters or breaches directly to the IPT etc.

Not addressed - The Bill does not introduce an obvious express power for the Investigatory Powers Commissioner to refer matters to the IPT. We have significant concerns with Clause 171 which, as drafted, confuses and conflates negatively the functions of the Investigatory Powers Commissioner and the IPT. Clause 171 also has significant implications with regard to the ability of individuals to seek effective remedy. Our concerns with Clause 171 are set out in detail in the next section, but a couple of points are worthy of mention here.

---

<sup>2</sup> See in particular, but not exclusively, sections 11 and 23 - <http://www.igis.govt.nz/assets/News/Inspector-General-of-Intelligence-and-Security-Act-1996.pdf>

Clause 171 interferes with, dilutes and limits significantly the very well established function of IOCCO to identify and investigate errors and of the Interception Commissioner to make determinations on errors and, where relevant, to inform individuals affected. Clause 171(11) provides that the definition of a “relevant error” will be described in the Codes of Practice. We do not have the draft Codes and therefore it is not possible to assess the detail of this important element.

We would like to make clear that we are seeking similar provisions for interception errors as we have currently for communications data errors (as set out in Chapter 6 of the current Acquisition and Disclosure of Communications Data Code of Practice). We also felt that it might be pertinent for the Investigatory Powers Commissioner to have the power to refer points of law to the IPT for interpretation where there is perhaps unclear or legally dubious practice. These are two distinct points.

- f. Expert resource to complement the Commissioner and inspectors – including technical, legal, privacy advocates, academics etc. Staff in the oversight body should be selected on the basis of expertise and experience. To complement the Commissioners’ expertise a wide range of skills is required – former law enforcement and intelligence agency officials, forensic experts, computer scientists, analysts, privacy advocates, lawyers and individuals with media / communications skills. This will ensure that the public authorities are robustly held to account and that all critical views are represented.

Partly addressed - The oversight impact assessment<sup>3</sup> published at the same time as the IP Bill does set out that technical and other skills will be required within the Investigatory Powers Commission. The budget set out in the impact assessment does represent an increase on the combined budgets for the current three RIPA Commissioners, but until the functions and structure of the Investigatory Powers Commission have been finalised it is impossible to assess whether the budget will be sufficient for the Commission to carry out the oversight effectively.

### **Clause 171 – Error Reporting**

9. Clause 171 is a paradox which requires substantial re-drafting and clarification to ensure that a) the delineation of responsibility between the Investigatory Powers Commissioner and the IPT is clear and, b) individuals are able to seek effective remedy. Our concerns are -

---

<sup>3</sup> [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/473777/Impact\\_Assessment-Oversight.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473777/Impact_Assessment-Oversight.pdf)

- Clause 171(2) – confuses the role of the Investigatory Powers Commissioner as an audit and investigation body with the role of the IPT as the means by which individuals can seek remedy where they believe they have been a victim of unlawful action under RIPA or human rights infringements in breach of the Human Rights Act 1998. As previously set out this provision dilutes and limits significantly the very well established function of IOCCO to identify and investigate errors and of the Interception Commissioner to make determinations on errors and, where relevant, to inform individuals affected. There is absolutely no need to interfere with that well established power, other than to extend it to interception errors. This cumbersome and unnecessary clause must be removed to ensure effective oversight and achieve greater transparency.
- Clause 171(2) - It seems illogical for the IPT to consider the seriousness of the error and its effect on the person concerned (essentially the merits of the case) before the person has actually brought a complaint to the IPT or the impact of the error has been established.
- Clause 171(2) - there is no definition of “*serious error*” and worryingly the definition appears to be solely dependent on the consequence of the conduct. The assessment of seriousness must have regard to the nature of the conduct itself.
- Clause 171(3) - the threshold for informing a person of any “*relevant error*” is extremely high. Will the Commissioner or IPT be able to determine if the error has caused “*significant prejudice or harm*” to the person concerned if neither are permitted to contact the person to discuss the matter.
- Clause 171(4) – noting our concerns regarding Clause 171(3) above we also note that the requirement for a serious error is that the breach must be more than simply a breach of a person’s convention rights (within the meaning of the Human Rights Act 1998). This threshold does not apply where an individual is seeking to bring an action to the IPT under Section 7 of the Human Rights Act where they merely have to show a public body has or may have acted in contravention of those rights. This is inconsistent and reinforces our concerns that the threshold is being set artificially high. Moreover breaches of Convention rights may be intrinsically serious as in the case of breaches for example of Articles 2, 3 and 5. The fact that there has been an unjustified disclosure of communications data or interception of communications does not of itself justify a finding of a serious error.
- Clause 171(11) – The definition of “*relevant error*” in the IP Bill does not relate to errors by CSPs as it is confined to errors by public authorities. In 2014, 38% of interception errors and 14.3% of communications data errors were attributable to CSPs. Clause 171(7) also only applies to public authorities.

10. No draft Codes of Practice have been published alongside the IP Bill and therefore it is not possible to understand how these provisions will work in practice. There are no error provisions in the current Interception Code of Practice. The error definitions and provisions in the current Acquisition and Disclosure of Communications Data Code of Practice will need to be amended substantially to align to Clause 171 and we have not had the opportunity to review those provisions.

11. Noting the importance of this clause to the entire oversight regime we are of the view that, due to its lack of clarity and the confusion of roles between the Investigatory Powers Commissioner and the IPT, it requires a complete re-draft.

**Clause 8 – offence of unlawfully obtaining communications data**

12. We have concerns that this new criminal offence will have the unintended consequence of undermining the open and co-operative self-reporting of errors and contraventions of RIPA and the Code of Practice by public authorities. There is a real danger that this provision could reduce accountability because the reporting process depends on individuals reporting to IOCCO at the earliest opportunity when they or their colleagues have made mistakes or when technical systems have failed. The criminal offence may deter some from reporting errors and lead to a subversive error culture. The criminal offence could reduce the shared desire by all parties to work together to resolve errors, prevent recurrence of errors and to strive for continuous improvement. It could perversely result in a greater impact upon an individual, or impact on a larger number of individuals, than might otherwise have been the case.

13. There is also a real risk that the introduction of this criminal offence will reduce individuals' and public authorities' co-operation with our investigations into any such errors or contraventions. For example, relevant persons whose conduct is questioned may refuse to answer questions or provide information to IOCCO in reliance on the privilege against self-incrimination.

14. There are examples in other legislation where such offences are treated as a collective act by a public authority, rather than an offence by an individual.

### **Prior authorisation & Post facto oversight**

15. There has not so far been much debate as to whether it is desirable for the same body to be responsible for the authorisation of investigatory powers and the post facto oversight of the exercise of those powers. The Committee may wish to consider this point.

16. If it is desirable to have both functions within the same body, then the Judicial Commissioners who are involved in the authorisation of warrants must be operationally distinct from those staff involved in the post facto audit and oversight of the public authorities. Otherwise this could be construed as the Judicial Commissioners “marking their own homework” which would dilute the credibility and independence of the new body. There would of course need to be considerable dialogue between the authorisation and oversight parts of the body to ensure consistency in approach and decision making. It will be crucial to ensure that the oversight section of the body is able to check properly that the information provided to the Judicial Commissioners in the applications was valid and that the subsequent conduct undertaken by the public authority aligned to the authorisation given. It will also be important for the Judicial Commissioners to draw on the technical and operational expertise of the oversight staff. This will provide the Judicial Commissioners with an understanding of the technical and operational aspects of the conduct they are authorising and assist them to consider properly the principles of proportionality and intrusion.

### **National Security Exceptions**

17. There appear to be a number of clauses which provide exceptions for national security or which exempt the intelligence agencies from key safeguards. It would be worth the Committee considering whether those, especially the combined effect, are justified. For example –

- Clauses 47(2) and (3) disapply the requirement for the designated person to be independent from the investigation when approving the acquisition or disclosure of communications data “in the interests of national security”. This dilutes the independence safeguard recently introduced into the March 2015 Communications Data Code of Practice (as a consequence of the *Digital Rights Ireland* case which resulted in a ruling by the ECJ).
- Clauses 60(2) and (3) disapply the requirement for the public authority to consult with a Single Point of Contact (SPoC) when acquiring communications data in the interests of national security. The SPoC is a key safeguard in the process.
- The justification for deeming the interests of national security always to be an exceptional circumstance is unclear.

- Clause 61 is designed to protect the confidentiality of journalistic sources but does not apply to the intelligence services. There is a wealth of case law setting out the importance of protecting the confidentiality of journalistic sources and the very recent judgement by the IPT (in the case of News Group Newspapers Ltd et al vs. the Commissioner of the Metropolis<sup>4</sup>) is also relevant to this matter. Is the exemption of the intelligence services from this provision justified?

### **Investigatory Powers under Part 2 RIPA and “other” Property Interference under the Intelligence Services Act 1994 or the Police Act 1997**

18. The Government has not taken the opportunity to bring all of the investigatory powers used by public authorities into the IP Bill. The result is that there are a number of inconsistencies and a lack of clarity in the authorisation processes in the IP Bill and those in Part 2 of RIPA (e.g. for directed and intrusive surveillance, covert human intelligence sources) and the Intelligence Services Act 1994 and the Police Act 1997 (e.g. interference with “other” property).

19. The IP Bill also curiously prescribes different authorisation and modification procedures for targeted equipment interference warrants made on behalf of the intelligence services or Chief of Defence Intelligence to those made on behalf of law enforcement (see for example clauses 84 and 87 vs. clause 89, clause 96). The different procedures are confusing and it is not clear on what basis they are justified.

### **Statistical Requirements**

20. The IP Bill Committee has asked if we are able to provide some further statistical information relating to interception warrants. In our 2014 Annual Report (published in March 2015) we published the total number of interception warrants issued, the total number extant at the end of 2014, the breakdown of warrants issued by statutory necessity purpose, and the total number of section 8(4) warrants issued. As we set out in our evidence to David Anderson QC’s Investigatory Powers Review<sup>5</sup> there are no statistical requirements in the Interception of Communications Code of Practice and the section 19 RIPA secrecy provisions make this area challenging.

21. The Committee has asked specifically if we can provide the number of interception warrants rejected by Secretaries of State. This is not a statistic we have required previously from interception agencies or warrant-granting departments on an annual basis. What we do require the interception agencies and warrant-granting departments to indicate to us during our bi-annual inspections are those warrants

---

<sup>4</sup> [http://www.ipt-uk.com/docs/IPT\\_14\\_176\\_H.pdf](http://www.ipt-uk.com/docs/IPT_14_176_H.pdf)

<sup>5</sup> [http://www.iocco-uk.info/docs/2014-12-5\(2\)%20IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf](http://www.iocco-uk.info/docs/2014-12-5(2)%20IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf)

which the Senior Official or Secretary of State have either rejected, or those which they have challenged or called for further information before authorising in the period under review (i.e. the previous 6 month period).

22. We have reviewed this information from the first round of interception inspections that took place in 2015 (covering a 6 month period) and have identified that approximately 50 interception warrants were subject to challenge or further information requests by the Senior Official or Secretary of State prior to them being approved. 3 interception warrants were refused in the period covered by those inspections. It is likely that these numbers will cover a mixture of new warrant applications, modifications and renewals.

23. We have previously commented that the rejection figure for interception warrants is inevitably low due to the high level of scrutiny that is applied to each warrant application as it crosses a number of desks in the interception agency and the relevant warrant-granting department before it reaches the Secretary of State. It is important therefore to note that the figure set out in the preceding paragraph does not capture the guardian and gatekeeper / quality assurance function carried out by firstly the staff and lawyers within the interception agency responsible for reviewing all submissions (prior to them being forwarded to the warrant-granting department), or secondly, the guardian and gatekeeper / quality assurance function carried out by staff in the relevant warrant-granting department prior to the warrants' submission to the Secretary of State.

24. The statistical requirements in the Acquisition and Disclosure of Communications Data Code of Practice were enhanced significantly in March 2015, but there are still no statistical requirements in the Interception of Communications Code of Practice. We would welcome the inclusion of statistical requirements into the Interception of Communications Code of Practice to improve transparency and accountability in this area.

### **Conclusion**

25. We would be very happy to provide the Committee with further information on any of the points in this submission, or indeed, on any other elements of the IP Bill.

- Ends -