EVIDENCE TO THE DRAFT INVESTIGATORY POWERS BILL COMMITTEE OF PARLIAMENT

Dr C. N. M. Pounder (Amberhawk)

12 December 2015

Introduction

1. This submission is primarily limited to the bulk personal dataset powers in Part 7 of Draft Investigatory Powers Bill ("***the Bill***") and other Parts of the Bill to the extent that they concern the processing of personal data (e.g. Part 3 deals with communications data that are also personal data – or "communications personal data").

2. My evidence assumes that bulk personal data collection powers will remain after the Committee has delivered its verdict; it thus suggests that a new structure that can introduce badly needed safeguards that are additional to the "double lock" (about which I make no comment and which I also assume will be maintained in any future Bill). The structure revolves around a new approach to the Data Protection exemption that applies for safeguarding national security and which has not changed since 1984.

3. In summary, I hope to show that **the Committee can assert that the Data Protection Act should become the prevailing mechanism that applies to the processing of personal data by the national security agencies**. In essence, this Bill updates the powers available to these agencies, but fails to update the protections afforded by the Data Protection Act. This is the major oversight addressed in my evidence.

4. The key changes that are needed to update the protection for individuals ("data subjects") and organisations are outlined below. They are:

    i. A separation between the Investigatory Powers Commissioner and the Judicial Commissioners to avoid a conflict where the Investigatory Powers Commissioner investigates himself or a judicial colleague.

    ii. The ability for organisations and data subjects to use an appeal system with respect to any warrant that requires the processing of bulk personal dataset for a national security purpose; for this to work, the separation in (i) above has to occur as it allows for an independent review of the warrant authorisation procedure.

    iii. A statutory Code of Practice that applies the Data Protection Principles to the processing of personal data for the purpose of safeguarding national security (rather than some proposed "Ersatz Principles" which in my view create a significant risk of "mission creep").

    iv. Detail on how the national security exemption (in section 28 exemption of the Data Protection Act) can be updated from the 1984 Act position; in summary, the exemption is applied when each warrant is sought or renewed and is specific to the warrant.

    v. The role of the Investigatory Powers Commissioner in regulating the Data Protection Act and the powers needed by the Commissioner to deliver effective protection for data subjects and protection for organisations subject to the powers in the Bill.

vi. For Government to clearly identify how Article 8 of the Human Rights Act is complied with; this is important given the Government's commitment to replace the Human Rights Act.

vii. A "sunset clause" on different Parts of the Bill, so the powers can be refreshed by Parliament in the context of future technological advances (e.g. the Internet of things); to do otherwise would leave a risk that broad based powers can be inappropriately used to legitimise activities that really should need Parliamentary approval.

viii. The removal of all powers that provide an alternative avenue to collect bulk personal data.

5. The protection afforded to data subjects by the Data Protection Act should be available even though the processing of personal data is for a very sensitive purpose. This is because *"the nature of the set is such that **it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service** in the exercise of its functions" (definition of a bulk personal dataset: Clause 150(1)(b)of the Bill; my emphasis).* Additionally, I suspect much communications personal data will also relate to many individuals who also prove to be of little interest to the national security agencies.

6. In short, if data subjects are "*unlikely to become of interest to the intelligence service"* then their personal data should be afforded, wherever possible, the full protection of the Data Protection Act by the Bill. My evidence shows how this protection can be delivered.

7. The Principles in the Data Protection Act have passed the test of time in establishing a balance between the need to process personal data for a controversial purpose and the protection of the interests of the individual concerned. For example, if the police and all their sensitive criminal intelligence collections of personal data about the Mafia can learn to co-exist with these Principles, without "mishap", for nearly three decades (since the 1984 Act), one cannot see why communications personal data or a bulk personal dataset held by the national security agencies should be any different, especially if the data subjects are "*unlikely to become of interest to the intelligence service".*

8. Since 1984, the national security function has been largely exempt from data protection considerations, as a wide exemption from the Data Protection Act applies whenever personal data are processed for safeguarding national security (Section 28 of the DPA). Evidence that this exemption applies can require a certificate to be signed by the Secretary of State; however this certificate, unlike a warrant, is only signed if or when it is needed.

9. Section 28 certificates appear to be timeless. This is illustrated by the Investigatory Powers Tribunal case involving Privacy International in October last year *([2014] UKIPTrib 13_77-H; delivered on 05/12/2014, paragraph 19*). In statements made to the Tribunal, the barrister for GCHQ produced a certificate signed by David Blunkett thirteen years previously (in 2001) to show that key obligations in the Data Protecting Act were exempt.

10. It is my evidence that application of the Data Protection Act in the way I suggest below could help mitigate concerns about the proportionality of collecting bulk personal datasets or mass communications personal data. This implementation applies the requirements of the Act to the national security purpose, it updates how the exemption for safeguarding national security is applied, and makes the Investigatory Powers Commissioner the

regulator who exercises the powers in the Act. It does not jeopardise the national security function.

11. The changes I suggest allows the Investigatory Powers Commissioner to:

    a. look into the detail of the processing of personal data for safeguarding national security purposes;

    b. deal with complaints from data subjects or data controllers;

    c. sort out proportionality problems associated with the processing of personal data. and

    d. where necessary enforce the appropriate data protection standards.

12. It is my contention that the changes I suggest establish a robust set of counterbalancing protections for data subjects and for those organisations that provide bulk personal datasets. **In a data protection sense, the Bill affords the opportunity to bring the national security agencies in from the cold**; **this opportunity should be taken**.

The Investigatory Powers Commissioner must be separate from the Judicial Commissioners.

13. My first comment relates to the Investigatory Powers Commissioner; this post has to be completely separate from the Judicial Commissioners who approve the warrants. **The Committee should consider recommending a separation between the Investigatory Powers Commissioner and the Judicial Commissioners.**

14. The Bill does not achieve any separation. Indeed, Clause 167(6) states that "*The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners*".

15. If there is not a complete separation between the Investigatory Powers Commissioner and the Judicial Commissioners, then the Government's chosen regulatory body is likely to be investigating the consequences of its own decisions. For instance, how is the Investigatory Powers Commissioner to meet the obligation in clause 169(3)(a) to *"keep under review the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service*" without investigating the consequences of his own warrant authorisation decision as a Judicial Commissioner (or any other Judicial Commissioner)?

16. In the context of national security and because personal data relates to a "*majority of the individuals are not, and are unlikely to become, of interest to the intelligence service*" the lack of separation inherent in the Government's proposals could easily undermine public confidence in the double lock protection, irrespective of the changes I suggest. This is likely to be the case, when in future, you have something akin to the Snowden revelations and an Investigatory Powers Commissioner investigating his own decision as a Judicial Commissioner.

17. As will be seen (at paragraph 41 below), separation is important to the success of the improvements I suggest. I also suggest that this separation will introduce an element of independence that will reassure the public about the collection of bulk personal datasets.

The Bill as drafted does not explicitly protect personal data

18. With respect to Part 7 of the Bill (the bulk personal dataset (BPD) provisions), paragraph 74 of the Bill's preamble (which appears under a heading "*What safeguards will there be*?") states that "*A statutory Code of Practice will set out additional safeguards which apply to how the agencies access, store, destroy and disclose information contained in the BPDs*". The BPD Code is proffered as a safeguard in addition to the "double lock".

19. However, in Schedule 6 which concerns all Codes or Practice, there is no detail as to what should appear in the BPD Code of Practice. **The Committee may wish to press for detail as to the content of the BPD Code as the safeguards appear to be no more than a blank canvass to be completed by the Secretary of State once a future Bill becomes law.** One cannot criticise the safeguards in the BPD Code if there is no Code or relevant provisions to make comments about!

20. However, the mere existence of this BPD Code of Practice means that the Government is anticipating the continuation of an unchanged wide Section 28 exemption in the Data Protection Act with respect of bulk personal datasets in favour of the Code (when its content is eventually published) – even though the personal data collected relate to data subjects of no interest to the national security agencies.

21. With respect to the processing of communications personal data in Part 3, there is another Code of Practice applying; the content of this Code is specified in Schedule 6, paragraph 3. Paragraph 3(2)(a)-(2)(f) contains what I would describe as "Ersatz Principles" (which do not apply to bulk personal datasets).

22. The Ersatz Principles in Schedule 6, paragraph 3(2)(a)-(2)(f) are as follows:

> "(*a) why, how and where the data is held,*
> *(b) who may access the data on behalf of the authority,*
> *(c) with whom, and under what conditions, the data may be disclosed,*
> *(d) the processing of the data for purposes otherwise than in connection with the purposes for which it was obtained or retained,*
> *(e) the processing of the data together with other data,*
> *(f) the processes for determining how long the data should be held and for the destruction of the data*".

23. These Ersatz Principles are phrased in a permissive way, unlike the Data Protection Principles. Clearly the intended function of these Ersatz Principles is to reassure the public; however, to the contrary, they fall well short of offering any significant protection.

24. For example, the Second Principle in the Data Protection Act requires that any personal data obtained for specific purpose(s) should not be further used or disclosed for an "*incompatible purpose*". By contrast, the Ersatz Principles (c) and (d) could allow for far wider uses/disclosure purposes by the national security agencies as the word "*incompatible*" is missing. Indeed any consideration of the "*purpose*" of any disclosure, which is crucial to several Data Protection Principles including the Second Principle, is absent from Ersatz Principle (c).

25. The Fifth Principle requires that personal data "*shall not be kept for longer than is necessary for that purpose or those purposes*"; the Ersatz Principle (f) clearly omits consideration of the "*purpose*" of retention and is inferior for that reason.

26. In general, these Ersatz Principles should be replaced by the Data Protection Principles that have protected data subjects for decades. In my view (and this comment might be uncharitable), the Ersatz Principles are not designed to protect the data subject; they are there to facilitate further processing (perhaps function creep) on the part of the national security agencies.

27. The Committee should assert that the Ersatz Principles in Code should be exchanged for the Data Protection Principles and that the Data Protection Principles should be central to all Codes relating to the processing of personal data.

How the Section 28 exemption in the DPA should apply

28. Clearly, there will be a need for exemptions from some provisions in the Data Protection Act that apply to safeguarding national security. I now show that the exemption can be wholly incorporated as part of the warrant arrangements and this step offers real safeguards for data subjects through a separate Investigatory Powers Commissioner.

29. In summary, the national security exemption is applied to the acquisition of bulk personal datasets or communications personal data ***when the agencies apply for each warrant (or on warrant renewal***) from the Secretary of State and a Judicial Commissioner.

30. Thus, instead of timeless certificates that are signed once, the exemption is applied for **each operation** at the warrant level (or on renewal or warrant) and at the time of the operation. In this way, consideration of the exemption from the provisions of the Data Protection Act becomes an additional protection to that of the judicial double lock. For example, the Judicial Commissioner and Secretary of State are able to consider issues such as further use, retention, lawfulness, accuracy, fairness and exemption from rights as part of the warrant approval process. In other words, the application of the Principles becomes central to the warrant authorisation process.

31. Residual Section 28 certification under the Data Protection Act may still be necessary for circumstances not covered in the Bill (e.g. there are limited to case-by-case exemptions that are necessary for the safeguarding of national security in any particular investigation). However, these certificates too should become time limited (e.g. 1 year before any renewal) and each application of this exemption should be covered by a certificate. The Investigatory Powers Commissioner should be able to review **all** aspects of the processing of personal data relating to such certificates even if they do not relate to personal data obtained from the use of powers in the Bill.

32. The enforcement regime (including Monetary Penalty Notices) in the Data Protection Act should apply to bulk personal dataset and communications personal data; such powers can be exercised by the Investigatory Powers Commissioner established by the Bill. The national security agencies right of Appeal against the exercise of powers by the Commissioner can be to the Investigatory Powers Tribunal.

33. This means that the Investigatory Powers Commissioner can obtain information about the processing of personal data, enforce the Data Protection Principles, consider the application of the national security exemption in detail, consider the rights of data subjects, and in the worst case scenarios, fine the national security agency if there is a serious transgression.

34. There is no risk to national security arising from such a safeguard but the fact that the data subject can seek redress via the Investigatory Powers Commissioner makes such redress accessible (unlike the current legalistic and costly appeal to the Investigatory Powers Tribunal).

35. The Assessment Notice power in Section 41A of the Data Protection Act to permit a data protection audit should be extended to apply to national security agencies in the context of bulk personal dataset and communications personal data processed by these agencies. If any Audit is undertaken by the Investigatory Powers Commissioner established by the Bill; there is no risk to national security arising from such a safeguard.

36. The Data Protection Act provisions with respect to data sharing should be applied. This usually means that any new data sharing has to be accompanied with a full Privacy Impact Assessment and can be subject to investigation by the Investigatory Powers Commissioner if need be. In general, there is no Privacy Impact Assessment accompanying this Bill even though most data subjects are not of interest to the national security agencies.

37. The data protection standards with respect to national security should be applied whenever personal data are acquired by the authorities. For example, clause 46(7)(a) of the Bill refers to obtaining personal data that are "*in the interests of national security*" which is lower than the data protection standard of obtaining personal data that is for "*safeguarding national security*".

38. Similarly clause 46(7)(b) refers to obtaining being "(*b) for the purpose of preventing or detecting crime*" when the data protection standard is that the person making the disclosure to the authorities has to be satisfied that "*failure to disclose would prejudice prevention and detection of crime*". (As a point of clarification; the more protective Data Protection Act provisions deal the exchange of personal data from the standpoint of the organisation making the disclosure; the draft Bill views the exchange from the standpoint of the authorities obtaining the personal data – however it is the same personal data that are being exchanged).

39. All the changes above would reassure the public that not only are the checks and balances at the warrant signing stage (the double lock), there could be independent checks on the subsequent processing of a bulk personal dataset and communications personal data at any time. The mechanism to trigger the checks and balances are available to data subjects and data controllers who have to provide the bulk personal data.

40. By contrast, there are no penalties for failing to apply the Code(s) of Practice that describe the processing of a bulk personal dataset and communications personal data and the only real checks occur when the warrant is signed or renewed. Indeed, there is no role for the Investigatory Powers Commissioner with respect to the Data Protection Act.

The role of the Investigatory Powers Commissioner

41. For the above to be successfully implemented, clause 169 should provide the Investigatory Powers Commissioner with the following powers and obligations to enforce the application of the Principles and where appropriate, rights of data subjects.

I. The Investigatory Powers Commissioner should exercise powers in the Data Protection Act with respect to bulk personal datasets and communications personal data in the same way as the Information Commissioner does in relation more normal personal data. Where the Investigatory Powers Commissioner exercises powers, these can be appealed to the Investigatory Powers Tribunal.

II. The Investigatory Powers Commissioner under the current Bill has no role in handling or investigating complaints from data subjects. As the majority of data subjects are "*not of interest*" to the intelligence services, the Commissioner should be able to consider complaints directly from them.

III. Organisations that are required to provide bulk personal dataset and communications personal data should be able to raise a formal complaint to the Investigatory Powers Commissioner that the warrant or authorisation approved by a Judicial Commissioner provides for disproportionate data sharing (i.e. organisations should have the right to ask for a review of a warrant/authorisation procedure if they have concerns over proportionality). To avoid prejudicing an operation, disclosure should first occur; however, any disclosed personal data should be destroyed if the Investigatory Powers Commissioner arrives at the same conclusion as the complainant (subject to appeal to the Investigatory Powers Tribunal).

IV. Consideration should be given for organisations and data subjects to appeal to the Investigatory Powers Tribunal against a failure of the Investigatory Powers Commissioner to find in favour of the applicant (using a process that was established for the Freedom of Information Act).

V. The Investigatory Powers Commissioner has no role in assessing whether bulk personal dataset and communications personal data, once approved under the warranting arrangements, have proved to be useful. The Commissioner ought to be able to establish Key Performance Indicators that demonstrate that bulk access is worthwhile (with the implication that if access is not worthwhile, the warrant becomes void and the datasets destroyed) and impose reporting requirements with respect to those Indicators on the national security agencies.

VI. All bulk personal dataset holdings should be reported to the Investigatory Powers Commissioner as well as the Secretary of State; this should be on the face of the Bill. This step will ensure the Commissioner knows the extent of bulk dataset collections and will be able to comment on these in his annual report, and where necessary exercise powers with respect to such personal data

VII. The Investigatory Powers Commissioner should have a role in supervising all Section 28 certificates under the Data Protection Act and ensuring there is no cross over with respect to powers in this Bill. (I have already stated that each application of the Section 28 exemption should be covered by a certificate which lasts a year to enable the certificate to be reviewed).

VIII. With respect to communications personal data obtained by authorisation (under clause 46 of the Bill), any authorisation has to describe why access is both necessary, proportionate and requires the application of any exemption in the Data Protection Act. The Investigatory Powers Commissioner should be able to define what detail he needs to be described and retained when authorisation occurs and what detail is needed to substantiate the use of each exemption in the Data Protection Act. The Investigatory Powers Commissioner should have the power to negate the application of any exemption in any particular case. Note: because of the range of

organisations involved with clause 46, there might be a number of exemptions in the Act that might apply that have nothing to do with safeguarding national security.

IX. Data matching across any combination of bulk personal datasets should be considered in the context of any data sharing to other bodies of the product of data matching. However, intended or actual data sharing and data matching should be identified in an authorisation, or on a warrant, or on warrant renewal, or reported to the Investigatory Powers Commissioner when a warrant lapses. The intent here is to allow the Investigatory Powers Commissioner to compile a complete picture of these activities and be able to investigate any data sharing or data matching arrangements.

X. The Investigatory Powers Commissioner can ensure that there is a commitment, as far as possible, to transparency with respect to bulk dataset acquisition/communications personal data. Such transparency already occurs without harm to national security. For instance with respect to Police & national security access Congestion Charge ANPR data, the TfL website states[1]:

> *"In 2012 the Mayor of London's Crime Manifesto included a commitment to instruct TfL to give the Metropolitan Police Service (MPS) direct real time access to the Automatic Number Plate Recognition (ANPR) cameras we use to enforce our Road User Charging schemes, for the purposes of preventing and detecting crime…..*
>
> *….**This was an expansion of a pre-existing arrangement with the MPS established in 2007, under which they were given access to TfL's ANPR data specifically for the purpose of using it to safeguard national security**. This arrangement was approved by the Home Secretary, who signed a certificate confirming that TfL, and the MPS, are exempt from certain provisions of the Data Protection Act 1998 for that purpose." (my emphasis).*

XI. The above shows that it is possible to be more transparent about the application of the Data Protection Act and the obtaining of personal data for their functions as clearly, if TfL's statement had jeopardised an operation, then the national security agencies would have asked for it to be removed.

Comments on Article 8 of the Human Rights Act

42. The Committee should recognise the Government is asking Parliament to accept that Article 8 of ECHR allows the national security agencies to collect bulk personal dataset and communications personal data when there is no prior suspicion with respect to the vast majority of data subjects. The legal advice that the Government has relied on to substantiate Article 8 compliance should be published so that this issue can be debated properly; at the moment, compliance with Human Rights obligations is asserted without evidence.

43. This is especially important as there might be changes to Article 8 that arise from the Government's review of the Human Rights Act, and of course, the purpose of the draft Bill procedure is to allow for such an informed debate.

44. **There should be a "sunset clause" on Part 7 of the Bill as Parliament needs to review the legislation in the context of future technological developments that**

[1] https://tfl.gov.uk/corporate/privacy-and-cookies/road-user-charging

will result in further bulk personal datasets being created (e.g. Internet of things, smart metering, ANPR datasets).

45. Parliament should learn from the abuse of process that arose by reliance on Section 94 of the Telecommunications Act 1984[2]. There are significant risks to allow wide ranging bulk data collection powers being left active for decades to come, to be used in any context, on any personal dataset, related to any future technology that might emerge.

46. I recommend **to the Committee a similar sunset clause in relation to communications personal data (Part 3) and to other Parts of the Bill.**

47. The Government wants the public to accept that the bulk collection of personal data does not breach their Article 8 rights without seeing the detail that justifies this course of action; such a leap of faith could be more palatable if the safeguards I suggest here were to be adopted.

48. **It should be a matter of policy that the more invasive the powers to interfere with private and family life, the stronger the powers of the Commissioner are to ensure that such powers are not misused**. Currently, with respect to the national security function, there is an inverse policy applying: the stronger the invasive powers, the weaker the protection for individuals. Sadly the proposals in the Bill continue the latter philosophy.

Removal of other powers to obtain personal data

49. All existing powers (i.e. other in the Bill) that could be used by the national security agencies to obtain a bulk personal dataset or communications personal data should be negated. For example, Schedule 1 of Counter-Terrorism Act 2008 which modifies the "Representation *of the People (England and Wales) Regulations 2001 (S.I. 2001/341*)" is not repealed. This modification includes Regulation 108A which is entitles the "*Supply of full register etc to the security services*". Not to close down existing powers would mean that there may be a secondary access route that could allow access to personal data outwith the protections in this Bill.

50. The powers to obtain bulk personal dataset are not limited in any way whatsoever; this means that bulk databases of medical records can become targets for acquisition. The Bill, however, protects privileged communications data, **the Committee should consider whether, for example, medical records need to be protected from the operation of the bulk dataset provisions**. If so, I recommend the inclusion of a defined set of databases that cannot be obtained in bulk and a general provision in the Bill that allows the Secretary of State to identify the bulk personal datasets that are protected.

51. Finally, there is a risk that the national security agencies could become a repository of bulk personal datasets that other public bodies can use. This risk is enhanced especially if the Data Protection Principles are exempted by wide ranging certificate under and

[2] The national security agencies have relied on pre-internet legislation (the Telecoms Act 1984) to legitimise activities that were never debated in Parliament. As the technology changed Government should have authorised in these activities in any anti-terrorism law from 2001 or indeed RIPA. This is evidence of a clear reluctance to engage with Parliament on these difficult issues.

unchanged Section 28 exemption (and if something like the Ersatz Principles appear as part of the BPD Code of Practice).

About myself

52. I have been a data protection practitioner for 30 years and am a founder member of Amberhawk Associates and a Director in Amberhawk Training Limited since the company was founded in 2008. The company specialises in training staff who are responsible for data protection, Freedom of Information, and information security and other aspects of Information Law.

53. In 2012, I was appointed to two Government Advisory Committees. I am a member of the Identity Assurance, Privacy and Consumer Advisory Group (advising the Cabinet Office on "privacy friendly" use of identity assurance techniques and on data sharing) and the Data Protection Advisory Panel (advising the Ministry of Justice on its approach to the EU's Data Protection Regulation and Directive in the field of law enforcement).

54. I have given oral and written evidence before various Parliamentary Select Committees where issues of privacy, data protection and security have arisen (e.g. ID Cards, Surveillance, Computer Misuse Act, data retention policies, supervision of the national security agencies). I have also been asked to give a presentation to European MEPs when the European Parliament was discussing the proposed Data Protection Regulation.

Dr C. N. M. Pounder;
Amberhawk Training Limited;
December 2015