Evidence to the Intelligence and Security Committee of Parliament

Dr C. N. M. Pounder (Personal capacity)

February 2013

Executive summary

1. The Committee should consider whether the Data Protection Act should apply to the processing of personal data by the national security agencies. Historically the national security function was made exempt from data protection by the 1984 Act (probably because this legislation predated the Interception of Communications Act 1985 or any consideration of any independent regulation of the national security function). This comprehensive exemption was carried over into the 1998 Act.

2. The Data Protection Principles have passed the test of time in establishing a balance between the need to process personal data for a controversial purpose and the needs to respect the needs of the individual. The national security function would benefit from the years of experience that data protection practitioners have in relation to performing such balancing acts. For instance, if the police and all their sensitive criminal intelligence collections of personal data can learn to co-exist with these Principles, without "mishap", for nearly three decades (since the 1984 Act), one cannot see why metadata held by the national security agencies should be any different.

3. There is no need to designate the Information Commissioner as a national security regulator. Disputes with respect to the application of the Principles can be tested by the National Security Tribunal which could hear complaints of substance; the Investigation of Regulatory Powers Tribunal could then assume the role of the Upper Tribunal and adjudicate on points of law. Any audit of compliance (like procedures with respect to warrants) could fall within the remit of the Surveillance Commissioner or the Interception of Communications Commissioner (as required).

4. The current set of Certificates which exempt the application of the Data Protection Act are sending the wrong message to the public; indeed I recommend the Committee requires the generic Certificates to be analysed by the Information Commissioner (the Government has put these into the public domain [e.g. in response to Parliamentary Questions, 25 Feb 2009: Column 867W] or FOI requests).

5. If the Committee decides against the application of the data protection principles to the national security function, the Committee should examine the **generic** Certificates to assess whether or not they are too widely drawn and recommend that they are published.

Substantive response

6. I have divided my substantive response into two parts. In Part 1, I answer the "fit for purpose" question (b), and in Part 2, I combine the response to questions (a) and (c).

PART 1: Response with respect to: b) "whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit for purpose', given the developments in information technology since they were enacted?"

Short Answer: "No"

A. The need for an alternative mechanisms of redress

7. There are limited means of redress in relation to national security function that an aggrieved individual can follow. These are:

    - ***Raise an issue with the Surveillance Commissioner or the Interception of Communications Commissioner.*** However, these Commissioners look at whether the Secretary of State and the national security agencies are using their powers appropriately and whether they have completed the relevant paperwork correctly; these Commissioners do not take complaints from individuals who are worried that they have been unjustly targeted as a subject of surveillance.

    - ***Take action under the Human Rights Act***; however, this exposes the individual to considerable costs if they lose the case. In the case of the national security agencies, the complainant takes on the State (e.g. the Home Office) backed by the tax-payer. This is a very uneven battle and a lengthy one – for instance, the mass retention of DNA (in *UK v Marper*) look six years to resolve.

    - ***Complain to the Interception of Communications Tribunal***: This is the forum where those who are seeking a hearing can get a Tribunal to look at the substantive issues. Because the Tribunal is not a public authority for FOI requests, there are no published statistics as to the number of complaints it receives. However, we do know the Tribunal publishes, on average, a single determination in a case per year. This suggests the evidential hurdles are high in bringing a case that is likely to succeed.

    - ***Raise an issue with the Intelligence and Security Committee (ISC) of Parliament***. This Committee was established in 1994 to examine the policy, administration and expenditure of the national security agencies; last year that it was given an increased remit to include oversight of operational activity and the wider intelligence and security activities of Government. In other words, the ISC's remit is more strategic rather than complaint driven (although multiple complaints on the same issue could easily fall within the ISC's remit).

8. As a general principle, the more the powers are invasive of individual privacy, the stronger the regulator should be in relation to protecting individuals when seeking redress. With

respect to the current arrangements that apply now, the stronger the powers of interference are counterbalanced with a reduced ability of seeking resolution to problems.

B The current national security certificates are sending the wrong message to the public

9. I have provided a reference to all of five Certificates that were published by the Home Office in 2005 in response to a series of FOI requests. I also have an analysis of the Certificate signed by Mrs May in relation to Transport for London in 2011; that too has been published. In total, seven generic Section 28 Certificates (including the TfL Certificate signed by Mrs May) can be downloaded from the references section at the end of http://amberhawk.typepad.com/amberhawk/2014/02/should-national-security-certificates-exclude-the-data-protection-principles.html.

10. I recommend that these generic Certificates be analysed by the Information Commissioner to confirm my analysis as I suspect the errors I identify below are endemic (Mrs May's certificate contains the errors in relation to the Second & Eighth Principles; it deals with the First Principle properly).

11. Looking at these five generic Certificates from 2005, there are common themes: a complete exemption from; the First, Second and Eighth Principles, the Section 55 offence, the Commissioner's powers of enforcement and the rights of access and objection. These latter exemptions from rights are understandable in the context of the national security function, and I will make no further comment on them.

12. In relation to the exemption from First Principle, it can be seen that only part of the exemption can be justified. For instance, the exemption from the need to provide a fair processing notice (giving a notice would be an act of "tipping off") and from "lawful" processing (e.g. obtaining personal data in breach of an obligation of confidence) can be justified.

13. However, the exemption from Schedule 2 and 3 requirements are difficult to see as being justified. For instance, any public body can process personal data which are "necessary" for its statutory functions which, in this case, is "necessary for the national security functions". It follows that an exemption from this obligation sends the message that the national security agencies might want the flexibility to process personal data that are "not necessary" for these functions.

14. Whether or not these agencies have processed personal data "unnecessarily" is at the heart of the Snowden allegations.

15. There is a similar "message to the public" with the exemption from the Second Principle. This Principle requires data controllers to obtain the personal data "lawfully" and not further process (i.e. use or disclose) these data for a purpose incompatible with the national security function. It follows that an exemption from this Principle implants the notion in the public that the national security agencies might want to process personal data for purposes that are incompatible with their national security function.

16. There again, this is an issue at the centre of the Snowden allegations.

17. Likewise with the message derived from the exemption to the Eighth Principle. This Principle requires a data controller to perform a risk assessment on the adequacy of protection, prior to the transfer of personal data outside the European Economic Area (EEA), or apply an exemption from the need to assess adequacy (see Schedule 4).

18. If these national security agencies were to make any transfer of personal data outside the EEA for a national security purpose, then such a transfer would normally be for a national security purpose and in the "substantial public interest" (and therefore qualify from an exemption to assess adequacy). It follows that message sent to the public is that the national security agencies require an ability to transfer personal data outside the EEA for purposes that possess little in the way of "substantial public interest".

19. In this context, the Snowden allegations concerning the personal data exchange between the NSA and GCHQ springs to mind; the USA is not seen as offering "an adequate level of protection" (certainly this stance is taken by many European Data Protection Commissioners).

20. Although the Certificates do not exempt the Third Principle (relevance) and Fifth Principle (retention), the exemption from Commissioner's powers means that any breach of national security agencies cannot be enforced.

PART 2: Response with respect to

a) What balance should be struck between the individual right to privacy and the collective right to security?

c) Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications?

Short Answer: I would change the legislation so that the Data Protection Principles apply to the balance between privacy and the collective right to security.

C Apply the data protection principles to national security

21. In summary, I cannot see why the national security agencies should not be required to comply with the data protection principles. For example, it would reassure the public if these agencies had, by law, to commit to the following obligations:

- Process personal data lawfully and ensure that any processing is necessary for their statutory functions.
- Ensure that personal data are processed in a way that is not incompatible with the national security purpose.
- Ensure that all personal data are adequate, relevant and not excessive in relation to the national security purpose.
- Ensure that personal data are kept no longer than necessary for the national security purpose.
- Ensure that personal data be kept secure

- Ensure that personal data are not to be transferred outside the EEA to a country that offers an inadequate level of protection unless there is a substantial public interest in any transfer.

22. Of course, there will be exemptions (e.g. from fair processing notices, rights of access or profiling; data sharing might need to apply the exemption from the non-disclosure provisions). What these exemptions are and their scope can be the subject of further debate.

23. One should add that these data protection principles have passed the test of time for 30 years or so. ***For instance, if the police and all their sensitive criminal intelligence collections can co-exist with these data protection principles for nearly three decades (since the 1984 Act), I cannot see why metadata held by the national security agencies are any different***.

24. I also cannot see why a regulator cannot investigate to reassure the public that these principles are central to the processing of personal data for national security purposes.

25. There is no need to have the Information Commissioner involved as a national security regulator. Disputes with respect to the application of the Principles can be tested by the National Security Tribunal which could hear complaints of substance; the Investigation of Regulatory Powers Tribunal could assume the role of the Upper Tribunal to adjudicate on points of law. Any audit of compliance (like procedures with respect to warrants) can fall within the remit of the Surveillance Commissioner or the Interception of Communications Commissioner (as required).

About Dr. C. N. M. Pounder

26. 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, information security and other aspects of Information Law.

27. 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).

28. He has also 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).

29. 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
February 2013