Witness:	Ailsa Beaton OBE
Statement No:	1
Exhibits Referred to:	AB/1
Date Statement Made:	29 March 2012

The Leveson Inquiry into the Culture Practices and Ethics of the Press

Witness: Ailsa Beaton OBE

Occupation: Director of Information

Address: c/o Metropolitan Police Service, New Scotland Yard

1. I have been asked to provide a statement for the purposes of the Leveson Inquiry. In preparing it I have sought to address all the questions asked of me in the Notice served pursuant to s.21 (2) of the Inquiries Act 2005. I begin each section of this statement by listing the questions to which I am responding.

(1) Who you are and a brief summary of your career history.

2. I am Director of Information and Chief Information Officer on the Metropolitan Police Service's (MPS) Management Board. My directorate provides information, communications and technology services to the 55,000 police officers, staff and volunteers of the MPS across 750 locations. I am also Head of the Information Management Business Area for the Association of Chief Police Officers for England and Wales, thus being a member of ACPO Cabinet and Chief Constables Council. I am also a Special Constable in the MPS. I

was awarded an OBE for my contribution to policing in the Queen's New Year's Honours 2010. I worked in accountancy after graduating but have now spent over 30 years working in a range of ICT roles. These have included being CIO for ICL plc, a senior partner with PA Consulting Group and undertaking various sales, management and technical support roles for General Electric (USA).

(2) Please identify the databases, owned and operated by the MPS, that hold personal/private information relating to individuals, for example intelligence databases. In respect of each database please explain (i) what broad categories of information are held on it; and (ii) who has access to it and for what purposes.

3. I exhibit to this statement as A/B 1, a file containing at tabs 1-5 documentation relating to the most prominent systems that hold personal/private information relating to individuals that have a core policing application. The systems are: -

<u>Crime Intelligence and Information System Plus (CRIMINT +)</u>

4. This is a system that provides access to, and searching of, linked MPS intelligence. This can be accessed by police officers, police staff and approved partners (e.g. local authority staff working in partnership with the MPS, or suitably vetted and approved contractors).

<u>MERLIN</u>

5. This is a system for the reporting of missing persons, children coming to notice of police, children taken into police protection, prostitute cautions, youth non-recordable offences, Child Protection Case Conferences and Sudden Deaths. It can be accessed by police officers, police staff, and possibly suitably vetted and approved partners.

Crime Reporting Information System (CRIS)

6. This system is used to report crime and manage the investigation through to conclusion. It can be accessed by police officers, police staff, station reception officers and approved partners (e.g. local authority staff working in partnership with the MPS, or suitably vetted and approved contractors.)

(3) How does information get placed on those databases? Who decides whether the information should be inputted?

CRIMINT +

7. Information is recorded on CRIMINT + by officers and the information is then reviewed by Borough Intelligence Units and CRIMINT + Core Administrators.

MERLIN

8. Officers create Pre-Assessment Checklist records whenever an incident they are dealing with directly concerns children, or if a domestic incident is attended and there are children present. Other records such as missing persons, sudden death reports and youth non-recordable offences are created by officers and staff on a "come to notice" basis.

CRIS

9. Crimes are usually entered by police officers and some staff in certain roles. Updates are carried out by police officers and staff. All crime reports are supervised and this is recorded on the report.

(4) How do users access the databases?

10. CRIS and Merlin are accessed via the MPS Corporate Network (AWARE). Users are required to enter a unique user identification and password in order to access AWARE. Currently to access CRIMINT + users are required to enter an additional user name and password specific to the application.

(5) How is access to those databases restricted and controlled? The Inquiry is interested in both technical and non-technical measures (such as instructions to users).

11. Access is granted to all systems based upon a user's duties. In order to obtain an account to use the systems the new user must be sponsored by a manager.

(6) What systems and/or measures are in place to ensure that information held on the databases is not misused? The Inquiry is interested in both technical and non technical measures.

12. All those who access the databases will be aware of the potential for their actions to be audited. This is made clear within the Information Code of Conduct, which is brought regularly to the attention of all staff. Please see Tab 1 - page 4.

<u>CRIMINT +</u>

13. The CRIMINT Support Team audit CRIMINT + as part of their remit. In addition local supervisory checks are required to be conducted.

<u>MERLIN</u>

14. A full audit capability recording record creation, viewing, changes and printing is available. Requests for audit enquiries are managed by the DOI Service Manager.

CRIS

15. Access to CRIS is auditable, and activity by a user within CRIS can be monitored. Audits can be conducted in relation to updates, transactions and enquiries run.

(7) Are individual users subject to any vetting procedures or security checks? If so, please give details. Is there a system in place for monitoring and reviewing the suitability of a person to have continued access to the databases? If so, please give details.

16. The MPS Vetting Policy requires all members of the MPS (police officers, police staff, and special constables), non-police staff (contractors, consultants and members of partner agencies) or any person having unescorted access to MPS buildings or uncontrolled access to police information to be vetted. Access to systems should be reviewed by line managers at the time of change of role or posting. Continued access to systems is reviewed during the course of any disciplinary investigations involving alleged misuse of systems / information. Please see the Vetting Policy at Tab 2.

(8) Are any restrictions placed on an individual user's ability to access information held on the databases (whether by technical means or by way of instructions to the user)? For instance, do some users have greater access rights than others? If so, describe the levels of access and to whom they apply respectively.

17. Role groups and security permissions are used to tailor individual user access and functionality. With CRIS access is controlled by permission levels within each user account.

(9) Are individual users permitted to browse the information to which they do have access without restriction? If not, what restrictions are in place and how are they communicated to individual users?

18. MPS systems and information may only be used for legitimate policing purposes. The MPS Information Code of Conduct describes to all users of MPS systems and information the use to which systems and information may be put. Please see the MPS Information Code of Conduct at Tab 1 - pages 2 and 3.

(10) What training is provided to individual users of the databases to ensure that they understand what is and what is not lawful/appropriate use of the information held on the databases? Who is responsible for providing this training?

19. For the relevant systems, training is provided through the national computer based training solution NCALT. The training must be completed before users can log on. Additional specialist courses are available.

(11) What systems and/or measures are in place to audit the use of the databases by individuai users? Describe the system of auditing, if any, that is In place.

20. See the response to question 6.

(12) What systems and/or measures are in piace (i) to prevent; (ii) to detect and (iii) to deter individual users of the databases from unlawfuily disciosing information?

21. All users undergo vetting before access is granted. Individual applications have their own training requirements and authorisation processes to ensure officers and staff granted access to systems have a legitimate business reason for access. All new users of the corporate information system AWARE are required to complete a mandatory computer based training package 'Computers and You'. Since the training package has been introduced, some 50,000 officers and staff have completed it. Please see the intranet notice at Tab 3. In addition users are made aware that they must comply with, amongst others, The

Personal Use of MPS ICT Systems SOPs at Tab 4 and the Information Code of Conduct SOPs at Tab 1.

(13) Do you consider that the systems and/or measures referred to in question (12) above work effectively? What changes, if any, do you consider should be made to them?

22. In my view the current proactive monitoring of system audit trails could be improved.

23. In an attempt to address the deficiencies, the MPS has procured the Huntsman product (from Tier-3) with a view to undertaking a pilot implementation of the software during the third quarter of 2012, followed if the pilot is successful, by a full rollout across the estate starting in the fourth quarter of 2012.

24. Huntsman is a Security Information and Event Management (SIEM) solution that provides proactive monitoring across the corporate ICT environment.

(14) In the last 5 years:
a. How many suspected unlawful disclosures have there been of information held on the databases to the media and/or private detectives?
b. How many investigations have there been into those suspected unlawful disclosures of information? What was the outcome of those investigations?

25. I have no direct knowledge of the answer to this question, so I asked the MPS Directorate of Professional Standards (DPS) for a response. They advised me that between 01/01/2008 and 29/02/2012, there have been 21 conduct matter cases involving 21 officers which have resulted in 25 officer allegations being recorded in relation to information leakage to the media.

26. A review of these 25 officer allegation summaries reveals that it has only been possible to identify one instance where a specific MPS system or database has been identified as involved in the leak. This related to information from Crimint + allegedly being leaked to the press. The allegation against the officer was unsubstantiated.

27. However, I am told that due to the interoperability of many of the MPS systems and databases as well as issues such as copy and pasting, note taking, duplication of information across systems, printing and photocopying, it is extremely difficult to pin down which database or system the leakage originated from unless there is a specific record/log number or transaction code attributed to the source.

28. DPS have indicated that some of the officer allegations are still under investigation and it is possible that misuse or leakage from MPS systems or databases is yet to be uncovered in these.

29. Of the 25 officer allegations, 4 have been substantiated, 12 are ongoing investigations and 9 were unsubstantiated. Of the 4 substantiated officer allegations, 2 resulted in dismissal (both of these officer allegations were for 1 officer), 1 in management action and 1 ended with no further action.

30. The DPS indicated that they have reviewed all 25 allegations for the period of 1st January 2008 to 29th February 2012 with a "Leakage to Other" flag to

identify if possible any that may relate to private investigators. I am advised that there are no incidents where a specific leakage to a private investigator can be identified.

31. With regard to members of Police Staff, I have relied on a response prepared by the MPS Police Staff Discipline Unit. They have indicated that:

    a) In the last four years no cases of police staff suspected of making unlawful disclosure of information held on databases to the media and/or private detectives have been recorded. [redacted]

    b) There have been no recorded investigations into those suspected of unlawful disclosures of information whereby information obtained has been disclosed to the media and/or private detectives [redacted] There has been a small number of further investigations of misuse of various MPS systems by police staff but there has been no evidence of disclosure of such information to the media and/or private detectives.

(15) Do you consider that the unlawful disclosure of information from the databases is a current problem? Please explain your answer.

32. Given the work that has been undertaken in this area by the DPS, I again have relied on them for providing a response to this question. They have indicated that the greatest risk to the MPS with regard to information misuse is by

persons authorised to see it who choose to pass it on, not those who access it illicitly.

33. They further indicate that intelligence databases are believed to be the main Systems utilised by leakers of information. Information leakage is integral to over two thirds of corruption investigations. Information is the commodity most valued by those who seek to corrupt MPS staff.

34. Information Leakage and Unlawful disclosure is a key strand of the MPS Professional Standards Control Strategy and an ACPO lead has responsibility for intelligence, prevention and enforcement activity.

35. The PNC is just one of a number of vulnerable systems but is subject to regular audit and additional dips sampling by professional standards.

(16) As regards the personal/private information held on the Police National Computer, what role does the MPS play in preventing, detecting and deterring its personnel (both police officers and civilian staff) from unlawfully disclosing such information? Please describe the systems and/or measures in place (both technical and nontechnical).

36. Please see the response to question 12. In addition all users of PNC must be trained to the appropriate level of competence. Use of the PNC by MPS officers and staff is monitored by the MPSPNC Bureau who perform random checks on a daily basis.

(17) What training is provided to individual users of the PNC to ensure that they understand what is and what is not lawful/appropriate use of the information held on the PNC?

37. The nature of PNC is described in the MPS PNC Standard Operating Procedure Paragraph 8 at Tab 5. Training on the user's responsibilities under the Data Protection Act and Computer Misuse Acts, together with the MPS Security Code (METSEC), and the Information Code of Conduct at Tab 1 must be delivered in all PNC training courses. This supplements the mandatory baseline training for all MPS officers and staff in the Computer based training package "Computers and You".

(18) What systems and/or measures are in place to audit the use of the PNC by MPS personnel? Describe the system of auditing, if any, that is in place.

38. The MPS PNC Bureau send out audit checks each day to the operator who carried out the search. Instances of potential misuse are raised with local Management, or in cases of serious misuse the Directorate of Professional Standards.

(19) Do you consider that the systems and/or measures referred to in question (18) above work effectively? What changes, if any, do you consider should be made to them?

39. It has been identified that line managers should also perform local supervisory checks in addition to those undertaken by the MPSPNC Bureau. This is a requirement of the PNC Standard Operating Procedure, but is not routinely followed. To address this monitoring of this requirement will be performed by the local Professional Standards Champions and a quarterly return made to the MPS PNC Bureau. The quarterly returns will be presented at the PNC Strategic Committee with a view to identifying specific issues and taking appropriate action if required.

(20) In the last four years:
a. How many suspected unlawful disclosures have there been of information held on the PNC by MPS personnel to the media and/or private detectives?
b. How many investigations have there been into those suspected unlawful disclosure of information? What was the outcome of those investigations?

40. Please see the answer to 14 with regard to Police Officers. With regard to Police Staff, I have again relied on the Police Staff Discipline Unit for a response. They have advised me that in the last 5 years:

a) There have been no recorded unlawful disclosure of information held on the PNC by police staff whereby the information been disclosed to the media and/or private detectives. There have been a very small number of abuses of the PNC by police staff but information has not been shared with the media and/or private detectives:

b) There have been no recorded investigations of unlawful disclosures of information held on the PNC by police staff whereby information has been disclosed to the media and/or private detectives. In keeping with the response given in a) there has been a very small number of investigations into misuse of the PNC by police staff but there has been no evidence of disclosure of information to the media and/or private detectives.

(21) Do you consider that the unlawful disclosure of information from the PNC by the MPS personnel is a current problem? Please explain your answer.

41. Please see the answer to question 15.

(22) Were changes made to any policies, procedures or systems relating to use of the databases and the security of the same following Operations Motorman, Glade and Reproof? If so, please specify.

42. No specific changes were made to my knowledge as a direct result of these operations. Nevertheless learning from these operations, and in particular Operation Glade, will have informed the Strategic Intelligence Assessment conducted annually by the DPS. This Assessment would inform how DOI's policies and procedures evolve.

(23) What additional measures, if any, should be put in place to prevent the unlawful disclosure of information held on the PNC and the MPS' own databases?

43. See the response to question 13.

<u>Further Information</u>

44. Further to the evidence provided by MPS Commissioner Bernard Hogan-Howe to the Inquiry on 20 February 2012 in which he revealed that all 55,000 police officers and staff were now permitted to access the Internet, I can add that my Directorate has commenced work to enable this change.

45. Currently approximately 39,000 officers and staff have access to the Internet. The policy limiting access to official use has only been relaxed where an individual's ability to complete their official or contracted duties is not compromised.

46. From April 2012 this access will be extended to all MPS officers and staff. As part of the preparations towards extending this access my Directorate has published interim guidance and has commenced activity to review existing policies and guidance in this space. Additionally I will be presenting costed

options to the MPS Management Board for the monitoring of our officers and staff online activity.

I believe the facts stated in this witness statement are true

Signed...[redacted]......................

Dated......29th March 2012....................