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

Witness:	**Jonathan STODDART**
Occupation:	**Chief Constable, Durham Constabulary**
Address:	**c/o Aykley Heads, Durham City**

I believe the facts stated in this witness statement are true

Signed**……** ***Dated*****……**

This is my second statement provided to the Leveson Inquiry into the Culture, Practices and Ethics of the Press.

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

Durham Constabulary owns and maintains sixteen main databases, which serve to assist in the day to day operations of the Force. The databases are used for various functions, for example, command and control or offender management both of which contain personal and sensitive personal data. Indeed the majority of our databases hold this type of data in very broad categories covering intelligence, crime and justice, public protection, personnel.

Access to the databases is granted dependent on operational need, and only those who require access for their day to day business to that particular

database will be granted role specific access rights. For example, cleaning and canteen staff do not require access to databases regarding intelligence, whilst operational police officers would not require access to payroll databases.

I have provided a more detailed summary of the databases to the inquiry, in document form, which includes the broad categories of data held on each and those who would be expected to have access.

2. How does information get placed on those databases? Who decides whether the information should be inputted?

The vast majority of data is submitted directly by police officers and police staff at their discretion, based on business guidelines with some oversight by my Data Management Unit (DMU) who assist in ensuring the quality of the data is to a high standard.

Data input is automated for some databases, such as Automatic Number Plate Recognition (ANPR) and other intelligence databases which take live feeds from other Forces and partner agencies.

3. How do users access the databases?

Access is granted by way of desktop personal computers (PCs) or laptop computers logged into the Force network. Users have to have a username and password (which must be changed on a regular basis for security).

Some testing is underway to establish the viability of more widespread remote access, but this is restricted to some of my senior managers at present.

Signed…….. Date……

4. **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).**

As already discussed, access to the Force network is controlled by username and password. Once on the network users must be members of the appropriate access group for the database they intend to access. Some systems have additional security in order for a user to gain access. Prior to accessing some databases users must attend a training session, for other databases, training is provided 'on the job'. Staff using databases are also appropriately and proportionately vetted.

Access is also restricted to some parts of some databases, on a need to know basis via the allocation of specific access groups.

5. **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.**

Quite simply this is about ensuring the right people have access to the right information for the right reason. This is done through restriction on access, education and enforcement. But ultimately there is an amount of trust and personal responsibility placed upon every user.

When any employee joins the organisation they are required to understand their obligations under the misuse of Force systems and data disclosure. They each read and sign a Security of Information form to this effect.

To reinforce this message prior to users being granted access to the network, they must read and agree to the system access usage statement which appears as a 'splash screen' for each and every log on. This explains to users

Signed…….. Date……

that systems must only be used for official purposes. I do not allow systems to be used for personal purposes.

All systems have audit facilities and my Professional Standards department conduct intelligence-led operations targeting individuals suspected of data compromise. The outcomes may include the naming of individuals who have left or been dismissed from the organisation as a result to reinforce to staff the importance of the integrity of data. More minor breaches which relate to poor performance rather than malicious intent or absolute neglect, are dealt with by way of advice and more general education to the wider organisation through Professional Standards newsletters.

6. **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.**

Since 2007 all new recruits and contractors with access to our network are vetted in line with the ACPO National Vetting Policy. Prior to this the full range of these checks was not carried out. Durham Constabulary formally approved the Force Vetting policy on the 14th June 2011. This means that existing officers and staff need to be re-vetted to bring them up to the standards set out in the ACPO Policy. Roles where specific risks have been identified, for example intelligence, have been completed as a priority, with only around 10% of the organisation yet to be vetted to this higher standard. This small delay is due to the organisational commitment to ensuring raised levels of vetting for our staff assisting with security for the forthcoming Olympic Games.

Annual vetting reviews will commence once all staff have gone through the ACPO vetting process.

Signed…….. Date……

Specific roles have been identified as requiring greater levels of vetting, these relating to the level of system access, the sensitivity of the role and the material that the person will have access to, for example vulnerability. Where a database contains information that is nationally sensitive, users may be required to undergo National Security Vetting (BPPS, SC / DV).

7. **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.**

As previously mentioned, access is restricted to some parts of some databases, on a need to know basis via the allocation of role specific access rights. These rights are based upon operational need. Police officers have the widest access rights, in particular to personal information for suspects, victims of crime and the wider information held on intelligence systems. This is appropriate in order to maximise their operational effectiveness in dealing with investigations, public protection and dealing with reported incidents. Indeed within the last three years we have increased the availability of data for a police officer to support this which I believe is reflected in the unprecedented levels of performance we have sustained during this period.

More recently I produced an internal 'webcast' which urged staff to consider the importance of data accuracy reinforcing the individual's responsibility when it comes to data.

8. **Are individual users permitted to browse the information to which they do have access without restrictions? If not, what restrictions are in place and how are they communicated to individual users?**

Signed…….. Date……

Generally if a user has access to a database there are no technical restrictions in place, however individuals should be well educated that such use must be for a policing or training purpose, otherwise it would constitute a misconduct or criminal offence. The communication of these restrictions has been covered in my previous answers through education and enforcement.

9. **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?**

This has been covered in my previous responses.

10. **What systems and/or measures are in place to audit the use of databases by individual users? Describe the system of auditing, if any, that is in place.**

Audits of all systems are conducted on an intelligence basis. Individuals can be monitored covertly through specific software, overtly and reactively through reviewing of transaction records of everything they have viewed on most databases. Each database operates on Locard's forensic principle that every contact will leave a trace.

11. **What systems and/or measures are in place (i) to prevent; (ii) to detect and (iii) to deter individual users of the databases from unlawfully disclosing information?**

This has been covered in my response to the above questions.

Signed…….. Date……

12. **Do you consider that the systems and/or measures referred to in question 11, above work effectively? What changes, if any, do you consider should be made to them?**

Potentially we could look to more proactively monitor our systems for example we could audit them in real time. For a small organisation like Durham Constabulary this could be achieved by an investment of around four staff, with additional resources, at an annual cost of £175,000. This, however, is not sustainable in the current climate of fiscal constraint.

A more cost effective method would be to involve the line management structure into the audit process so that managers are responsible for auditing the majority of the work done by their staff. Arrangements are in hand for this change to be scoped, prepared and implemented.

13. **In the last five years:**

    a. **How many suspected unlawful disclosures have there been of information held on the database 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?**

I am not aware of any suspected leaks from Durham Constabulary databases to the media or private investigators within the last five years.

In a non-media specific sense, there have been nine investigations conducted by my Professional Standards department into suspected data compromises of local databases by both police officers and police staff. Two of these cases are currently live. The remaining seven have been finalised and are all very

Signed…….. Date……

different in their nature, but all hold the same common thread, that the information was accessed without a genuine policing purpose.

The following action was taken against the officers and staff in these cases: one case was not proven, and no further action was taken. Two cases resulted in criminal proceedings and those involved received simple police cautions; in both of these cases the police officer and member of police staff resigned from the organisation. Another three investigations resulted in final written warnings for police officers at misconduct hearings. More recently a Police Community Support Officer resigned prior to an investigation into data she is believed to have passed to a friend who was a relative of a murder victim.

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

Any compromise of data is a problem, and has the potential to harm an individual based on the personal or sensitive personal data held regarding them. An enormous amount of trust is placed in Durham Constabulary as a public body to safeguard this information, and I think my response to the previous answer demonstrates how seriously such breaches are treated.

When considering the millions of data transactions Durham Constabulary carries out each year we do not appear to have a large scale problem. I believe a good indicator of this is the small number of public complaints received by my Professional Standards department about data compromise, which in effect is only two in number in the last five years. One of these cases was reviewed by the Independent Police Complaint Commission and ruled to be vexatious.

Signed…….. Date……

15. **As regards the personal/private information held on Police National Computer, what role does Durham Constabulary 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 non-technical).**

Durham Constabulary uses a technical system called PNC Guard supplied by a private company. This system can be used overtly or covertly and is administered centrally within my PNC liaison team. The overt PNC Guard system uses random live audit requests prior to the user being able to progress to the PNC record. These live audit requests are reviewed retrospectively by my PNC liaison team who may request further information to ensure the check was legitimate and for a policing purpose. Any suspected breaches are referred to my Professional Standards department for a more thorough investigation.

There are occasions when a non-technical request is sent to a PNC user to ascertain why PNC records were accessed – this can be in response to a pop up received, or can be via a random check of the Transaction Log, whereby a form will be sent to the user to request details of why the check was completed – the form must be signed by the users supervision.

PNC users are also vetted for usage on the system, as per the PNC Code of Connection. The PNC logon screen also has a warning to users informing them that unauthorised access or misuse of the system is prohibited.

Once again, as with any system where a 'human being' is involved, there is an amount of trust and personal responsibility placed upon them.

Signed…….. Date……

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

All users of PNC must complete training to allow them to access various elements of data within, for example persons or vehicles. During training all students are reminded of the appropriate legislation which includes:

The Data Protection Act, The Computer Misuse Act, The Copyright, Designs and Patents Act, and the Criminal Justice and Public Order Act.

Trainers will give examples of what is lawful/appropriate usage and what is not. At the end of the PNC course students are required to sign a 'Proper use declaration' which again sets out what is lawful/appropriate usage and what is not.

17. What systems and/or measures are in place to audit the use of the PNC by Durham Constabulary personnel? Describe the system of auditing, if any, that is in place.

This has been covered by my response to question 15.

18. Do you consider that the systems and/or measures referred to in question 17, above work effectively? What changes, if any, do you consider should be made to them?

The current PNC audit facility within Durham Constabulary is, in my opinion, effective. My Force Information Auditor has for the last four years regularly attended meetings of the ACPO National Data Quality Audit Group, which shares good practice from other Forces on the audit of PNC and where

Signed…….. Date……

national risks and threats are discussed. Our five year audit plan reflects national practice.

This collaboration has led to us adopting a more rigorous approach to auditing, for example the adoption of the PNC Guard system.

19. In the last five years:

a. **How many suspected unlawful disclosures have there been of information held on the PNC by Durham Constabulary personnel 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?**

Once again I am not aware of any suspected leaks of PNC data from Durham Constabulary employees to the media or private investigators within the last five years.

There have been two investigations into the unlawful disclosure of PNC data by Durham Constabulary officers and staff within the last five years. The first case relates to an officer who was requesting checks by colleagues who were unaware these checks were for his own use. This officer was initially dismissed after a misconduct hearing, but reinstated on appeal, receiving a fine by the Police Appeals Tribunal. The second case related to two officers, one who was the PNC operator and a colleague requesting details for his son to streamline a visa application. Both of these officers received management advice which was proportionate in this case.

Signed…….. Date……

20. Do you consider that the unlawful disclosure of information from the PNC by Durham Constabulary personnel is a current problem? Please explain your answer.

Similarly as the response to question 14, any unlawful disclosure from PNC is a problem but I do not believe Durham Constabulary does have such a problem, this is in part due to the relative size of the Force and volume of PNC transactions and I am confident that any large scale or systematic problems would be swiftly identified through audit as a result.

21. 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.

Durham Constabulary reviewed and replaced our policy for Notifiable Associations. This policy advises staff on when they need to notify the organisation of an association or friendship with someone who could pose a risk of compromise to that individual. Of particular note is the application of the current policy to private detectives.

The recommendations from the Information Commissioners Office were also the catalyst for the streamlining of an online internal confidential reporting system called 'Bad Apple', as well as the procurement of an improved covert audit and monitoring system.

22. What additional measures, if any, should be put in place to prevent the unlawful disclosure of information held on the PNC and Durham Constabulary's own databases?

Firstly, there are opportunities for my Professional Standards department to enhance their audit capabilities to detect misuse through an updated system.

Signed…….. Date……

Secondly the Force requires a better understanding of the private detectives operating in our police area. An assessment is currently underway as to how to best achieve this, but one of the risks to be addressed is; are any of them retired officers, who could use contacts within the Force to attempt to source PNC or other Force data? It is hoped that armed with such knowledge we would be able to more proactively protect current employees from compromise and thus maintain the integrity of data held.

Additionally it would be useful for clarification on the level of action recommended when data compromises do occur. Such advice could include a threat and harm matrix. The level of action, or indeed inaction, is currently left to individual Forces to decide; whilst Durham Constabulary has maintained a common sense approach, a more consistent sense of national direction would strengthen the preventative message.

Signed…….. Date……