IN THE MATTER OF

THE LEVESON INQUIRY

STATEMENT OF MARK ALAN HUGHES

I, Mark Alan Hughes of 81 Newgate Street, London EC1A 7AJ will say as follows:-

1. I am currently employed by British Telecommunications plc ("BT") as the Managing Director of BT Security. I have held this position for approximately five years. In this role I have responsibility for all of the security in BT.

BT General Security Policy

2. Security within BT is primarily concerned with the protection of customer, supplier and BT information, safeguarding its people and assets, protecting its operations, responding to and investigating security lapses and reducing the cost of security failure. The BT information security management system for the co-ordination and development of BT security policies has been awarded certification to ISO/IEC27001.

3. BT publishes its Security Policies and Practices on the BT Intranet. All BT people have a personal responsibility to ensure that the security arrangements for themselves, the people they manage and the

premises in which they work, are all fully understood and complied with.

4. All BT people are required to familiarise themselves with, and implement, the relevant Security Policies and Practices that apply to their job and responsibilities. They are informed that breach of a Security Policy is a disciplinary offence, which can result in dismissal and, in some cases, lead to criminal prosecution.

5. All BT people are required to complete a mandatory course "Security in BT" upon joining BT. This Computer based training includes information on internet and email, personal, vehicle, systems, laptop, travel and home worker security. Completing it ensures that BT people have a basic understanding of the security needs of the company and what they need to do to keep BT, its people and its customers safe and secure. The course introduces the risks associated with protecting buildings and access, protecting information, protecting information technology and protecting people and shows people how to avoid those risks by adopting recommended security behaviours or following approved security processes. Thereafter BT people must complete an annual security checklist to ensure continued compliance with the policy.

   (For copy extracts from Security Policy, details of mandatory training and social engineering see Appendix 1).

   Social Engineering

6. BT has come across social engineering. In general terms, we regard this as criminal activity, intended to procure personal information, usually by manipulating other people into disclosing that information unlawfully. BT is most commonly targeted by two broad forms of social engineering: a) fraudulent calls to BT Customer Contact Centres purporting to be from an account holder and attempting to obtain

confidential account information (in particular relating to bank accounts); and b) fraudulent calls to other BT employees where the caller purports to be a BT employee and attempts to illicit confidential information regarding the Company, its practices or other employees.

7. All the reported security incidents concerning social engineering are referred to BT's Crime and Investigation Services team for formal investigation. Each case is allocated a unique case reference number and assigned to an appropriately qualified Investigation Specialist. BT operates, and has for many years, an information retention policy. BT's information retention policy is attached at Appendix 2. This policy states that Security Investigation cases should be kept for 6 years or until the end of the custodial sentence (if appropriate). Consequently we are not able to go back to 2001 as requested in the letter to me dated 13 October from the Assistant Solicitor to the Inquiry. Accordingly, information regarding cases older than this period is not available. The topic of information retention is dealt with in more detail below at paragraphs 11 to 12.

8. In response to the letter to me dated 13 October from Khaleel Desai, Assistant Solicitor to the Leveson Inquiry, I coordinated a review of our security case records concerning social engineering over the past 6 years. The review concluded that there has been one reported potential social engineering incident that we were able to identify as obviously media-related. This potential incident came to light in August 2006,

9. The review I refer to in paragraph 8 above also concluded that there have been 19 cases involving social engineering in the last 6 years that were sufficiently serious to have been dealt with by BT Security

investigations and the discipline duty of BT. Details of these cases are set out in Appendix 3.

10. For a number of years BT notified social engineering incidents to the Information Commissioner's Office (ICO) in accordance with a Memorandum of Understanding (MoU). That MoU expired in May this year and we are now seeking to renegotiate it in the light of new data protection reporting requirements. The results of the ICO's own investigations into the cases we refer to them are in due course reported to BT, but they do not notify us of the context of the cases. The cases which BT Security has notified to the ICO during the last 6 years are included in the table at Appendix 3. They are clearly identified by the explanation in the "Notes" column. There are other disciplinary cases involving BT staff, for example a customer complaining regarding the attitude of an employee listed against unauthorised access of CSS data these have not been included in this list.

Information Retention

11. As previously mentioned in paragraph 7, BT has in place a clear policy on Information Retention ("the Policy"") a copy of which is contained at Appendix 2. It sets out the requirements for information retention and the disposal of information. It is mandatory for all BT Business Units to comply with the Policy.

12. The Policy is owned by the BT Group Governance and Compliance Department and covers all information of any kind (text, data, voice or visual image). It states that information should be retained for no longer than the recommended maximum of two years unless a different retention period is specified in the Schedule to the policy. The Schedule to the policy can be found at Appendix 2, the applicable data retention period is at page 42. It contains a list of documents and

information items that must be retained for specified periods of time for legal, statutory, fiscal, historical or operational reasons.

Data Protection

13. BT takes its data protection responsibilities very seriously. As many BT people may have access to and process the records of customers, suppliers or colleagues, it is imperative that they understand and comply with data protection and related legislation relevant to their business activities. Accordingly, in addition to the General Security training, we deliver mandatory training for all BT staff, both in the UK and abroad.

14. In particular, all UK-based BT managers must complete a course entitled "Data Protection: Handling with Care" every two years to ensure awareness of the subject is maintained. The basic aim of this course is to explain how to handle personal data appropriately and how to keep it secure. All team members (ie non managerial grades), BT contractors and agency personnel must complete the "Basic Regulatory Compliance for team members" intranet training which also includes a section on Data Protection. This must be repeated every three years.

15. Newcomers to BT (new recruits) are required to complete the mandatory training appropriate for their role within 30 days of starting with BT. Employees and agents who will be customer facing, including those recruited as Call Centre Agents (ie those people who are most likely to be targeted for the purposes of illegally obtaining personal data), should complete this mandatory training as part of their new entrant training prior to contact with customers/customer data. The training is computer based and consists of learning modules followed by a proof of learning quiz. It is provided through a computer system which emails individuals to remind them when their training is due. In addition BT has a Regulatory Compliance team which chases people

up to ensure that they complete the training within the timescales. We typically have a 95% completion target by the end of March each year, and records suggest that this is constantly surpassed.

16. These formal training courses, which are designed to provide an overview of data protection and related law, are supplemented by a wide range of additional material, some of which is tailored for particular audiences and some of which relates to particularly important or topical items. In January last year BT launched a Data Protection awareness campaign called "Think Privacy!" This campaign contained clear and straightforward messaging on a range of issues, together with messages from senior managers. The campaign was subsequently refreshed in November last year and will be again from time to time going forward. The associated Think Privacy! website has been retained and is regularly updated.

17. The majority of bespoke training/awareness material has been prepared for BT's Retail Division, which provides products and services to our mass-market consumer base in the UK. We believe that it is particularly important to ensure that all employees within BT Retail's Consumer Business Unit and especially those who are in frequent contact with customers and who have access to and process customer data, are fully aware of their data protection responsibilities and of the dangers posed by social engineering. Examples of role specific training material provided to BT's retail staff can be found at Appendix 4.

18. BT's Data Protection Task Force (DPTF) reinforces the Company's rigorous approach to data privacy and control. A description of the DPTF's responsibilities is at Appendix 5. BT's Personal Data Breach Process is at Appendix 6).

19. BT's internal security procedures and policies give specific advice regarding social engineering (see Appendix 7). Additionally, staff working for BT's main customer facing business units (BT Retail and

BT Wholesale) are also provided with further separate advice regarding social engineering. Copies of these policies are contained at Appendices 8 and 9 respectively.

20. Further, ad hoc briefings are provided to employees covering other aspects of account security, in particular to remind them that details of any caller who does not appear to be genuine should be flagged to the line manager and BT Security. A formal matrix stating the Data Protection training requirements across the business is at Appendix 10.

21. Further, BT's mandatory regulatory compliance training for contractors requires that those contractors with access to personal data must complete Data Protection and Privacy training.

Systems Access Security

22. BT has many business systems that contain information critical to its operations. BT has a general policy on Systems Access Security.

23. The Policy requires that systems should be designed to ensure in particular that; access to services is via a secure logon process; access is limited to the minimum number of users and enforces the 'deny all' principle unless access is specifically allowed.

24. This means that access to these systems must only be given to those who need it to do their job. The policy provides that individuals granted access to an application/computer system must be briefed by their manager on their security responsibilities within 7 days of the access being granted. They must indicate by signature or email, their agreement to be bound by their access rights and responsibilities before they are allowed to access the system.

25. BT regularly sends out communications/briefings to remind BT people of their security and data protection obligations. These are delivered either by email, by posting on the intranet or are published in

newsletters or internal publications such as BT Today (a magazine sent to all BT people) or PeopleNews.

26. BT's customers are its biggest asset and BT is committed to protecting their data. Many of the people BT employs require access to customer data in order to carry out their roles. BT is of course reliant on its people to comply with its Policies and Practices and has to place a certain degree of trust in them. Since 2004 BT includes criminal record checks in its pre-employment checks for all new recruits. BT imposes controls on who has access to the data, and provides those who do have access with specific instruction and training on the use of the data. This is reinforced by reminders, briefings and refresher training. Please see Appendix 11 for an example of a reminder used when accessing various systems and the additional warnings posted on our website. BT takes its responsibility to protect customer data very seriously and will not tolerate misuse of its systems or inappropriate or unauthorised access. For this reason BT ensures that user access can be tracked so that any misuse may be detected and offenders can be dealt with appropriately. BT constantly reviews and strives to improve its practices.

Signed .....

Dated .....