Witness Statement

1. I, Simon Tse, Chief Executive Officer of the Driver and Vehicle Licensing Agency, Longview Road, Swansea, SA6 7JL declare as follows:

2. I am Chief Executive Officer of the Driver and Vehicle Licensing Agency (DVLA), an Executive Agency of the Department for Transport (DfT). I have held the post of Chief Executive Officer since May 2011. Since I joined the Civil Service in 2008, and previous to my present post, I was the Chief Operating Officer (2008-2010) and Acting Chief Executive Officer (May 2010-May 2011).

3. I make this witness statement to assist the Leveson Inquiry into the cultures, practices and ethics of the press.

Background

4. The DVLA has its headquarters in Swansea and has a network of 39 offices around Great Britain. It plays a key role, working with the Police and others, to keep road users safe by:

- Maintaining over 44 million current driver records and 36 million current vehicle records, handling around 200 million customer interactions each year as a result collecting nearly £6 billion a year in Vehicle Excise Duty (road tax).
- Limiting road tax foregone through non-compliance to no more than 1 per cent.
- Supporting the Police and other enforcement bodies in dealing with crime.

5. The DVLA holds information on two separate registers. The vehicle register is maintained primarily to identify vehicles used on public roads, to assist law enforcement and the collection of taxes, and to facilitate improved road safety. It holds information about each motor vehicle (e.g. registration mark, vehicle identification number, make/model, emissions, etc) and includes the name and address of the registered keeper, dates of acquisition and disposal of the vehicle, and the status of vehicles as to whether they are licensed (taxed) or declared off road (SORN).

6. The driver register holds each driver's name, address, date of birth, photograph (where a photocard licence is held), driving entitlement, motoring convictions and

current penalty points, together with information about medical conditions relevant to driving.

7. Subject to a range of controls, access to vehicle and driver information is possible via paper, telephone and electronic channels. Information from the vehicle and driver registers is disclosed to third parties where legal powers allow or require this or where the data subject has given their consent. I have arranged for a search of the DVLA records in relation to the blagging of information and the unauthorised release of information by DVLA staff members.

Identified attempts to blag information from the DVLA

8. There is some evidence that the DVLA has been targeted by persons seeking to blag information held on the vehicle and driver registers. Over a period of 10 years a small number of these attempts have been identified. All have been via telephone or paper channels. It is not possible to be certain but it appears that none of these instances have involved disclosure of information directly to the media. The incidents I am aware of are referenced in the list of attached documents numbered 1-4. These are internal DVLA intelligence reports which use the format of the National Intelligence Model in use by the Agency to help prevent the abuse by criminals of its products and services. The reports have been anonymised for the purpose of this witness statement.

9. The attempts have not been particularly sophisticated and would appear to have been isolated rather than systematic incidents. For example, the caller/writer provides sufficient information to convince the clerk that s/he is eligible to obtain additional information from the record. The information contained in these intelligence reports was passed to the Police at the time for their consideration of appropriate action.

The value of information held on DVLA records

10. Whilst the primary function of the driving licence is to convey entitlement to drive, it is widely accepted and used in support of identity in a range of circumstances. There may be road safety implications if individuals with no entitlement to drive are able falsely to obtain genuine licences or use information to produce convincing counterfeit licences.

11. Access to driver data by criminals could enable them to make fraudulent applications for driving licences, produce counterfeit licences which contain details of another individual, or use the personal data to access other services, for example to use the licence as evidence of identity to apply for credit.

12. Data from the vehicle record could be used to clone a vehicle. Cloning is a process used by criminals where the identity of a stolen vehicle is changed to that of a similar genuine vehicle. Information about the genuine vehicle could be used to apply for a vehicle registration document (V5C) for the clone, giving the criminal a genuine document to support its onward sale. The data on the vehicle record could also be used by a criminal to produce a counterfeit V5C document, containing details of a genuine vehicle, which could then be used to support the sale of a stolen vehicle in the same way. The information needed to apply for the V5C is in most cases available by other means. For example, where the genuine vehicle is available for sale, criminals are known to pose as consumers to obtain the information from the vendor.

13. The attempts at obtaining information show that the blaggers already have a reasonable amount of information about the individual or vehicle targeted in order to overcome the security procedures in place. Both British and foreign nationals are believed to be involved in these attempts, however specific information is not held by the DVLA.

Safeguards and controls to prevent unauthorised disclosure of DVLA data

14. The DVLA takes its obligations for the protection of the information held very seriously. As a customer-facing organisation, the Agency must make services and information easily accessible to customers. All staff have workplace induction training when starting their employment at the Agency including briefing on the security of data (*document 5*) and must complete an Information Security Training course annually.

15. Customers have a choice about how they approach DVLA for data – electronic, telephone and paper channels. Each channel has specific processes to safeguard information whilst providing accessible and cost effective services.

16. There is a process for assessing all requests from companies to access DVLA data electronically. Appropriate information assurance and IT controls are in place to ensure data is provided only to known contacts. These controls are comprehensively documented and can be provided on request should this area be considered relevant to the inquiry.

17. Staff managing telephone enquiries in the Contact Centre are required to read and sign a Security Document (*document 6)* on an annual basis. This document refers staff to a relevant desktop security guide (*documents 7 and 8)* advising clerks on the release of information from the driver or vehicle record. The guide indicates what information needs to be provided by the customer to satisfy the clerk of their identity before any information is disclosed. If the clerk believes that a bogus caller is attempting to access information the other clerks are alerted by way of scrolling information screens visible to all call handlers and by alerts on the Agency's Intranet home page visible to all staff as they log into their computers.

18. Applications for driving licences and vehicle licences can also be made online. Safeguards are in place to ensure that the correct person will be in receipt of a driving licence. For a first application for a driving licence (where there is no driver record), the applicant must provide their full name, date of birth, 3 years previous address history and supply personal 'secrets'. They may also supply their passport number and National Insurance number to allow checks to be made with the Identity and Passport Service (IPS) and the Department for Work and Pensions (DWP) respectively. This information is not mandatory. Checks are made with IPS, DWP and /or an external commercial information broker.

19. During this process the customer accumulates a 'score' using a decision engine, if the score is high enough and DVLA is confident that they are who they say they are (based on the E-Government Strategy Framework Policy guidelines for online authentication level 2), for those customers a driving licence is issued. For customers who don't achieve a high enough score, no licence is issued until they provide us with the further evidence required. These second stage applications are received via the postal route.

20. For existing licence holders the system will ask for the same information plus driver number. An additional measure is to check this information against the driver record held. The customer details must be an exact match to the driver record. If there is more than one possible match to a driver record, the customer cannot

continue with their application. Customers cannot change name on-line, this is a postal application only.

21. All paper enquiries seeking information about registered keepers of vehicles must be submitted on the relevant enquiry forms. Customers must supply proof of identity and address, to help ensure DVLA is releasing data securely to the correct person.

22. Written vehicle enquiries must also supply supporting evidence depending on the nature of the enquiry to show that release of the data complies with the legal gateway to release information under the reasonable cause provisions. A matrix setting out these provisions is attached (*document 9*).

23. The declaration on these forms must also be signed. It states that the information supplied on the application is true and that a criminal offence is committed should data be obtained fraudulently.

24. To obtain any information from the driver record via the paper channel, the full name of the driver, the date of birth, their address as recorded on the latest driving licence issued and the driver's signature must be provided. All these details are checked against the record held. Where discrepancies are found, the application is rejected.

25. Together with initial training received by all staff, ongoing information about Data Protection is available on the Intranet and there is a dedicated Data Protection team which advises the Agency's staff about the release of personal data.

Unauthorised disclosures of DVLA data to third parties by DVLA staff

26. There have been instances within the last 10 years where staff have been disciplined for disclosing information from driver and vehicle records. DVLA is not aware of any instance where a member of staff has been dismissed for disclosure of information directly to the media. In one case, I know that information was obtained by a private investigator who then supplied the information to the press. This case was referred to in the Information Commissioner's 2006 report "What Price Privacy?" A brief summary is provided in document 10, though DVLA retains more detailed case papers on this matter which can be made available upon request.

Confidentiality

27. In order that the DVLA may maintain the integrity of its procedures against criminality, I ask that the contents of this witness statement and the associated documents be treated as confidential. If information about the DVLA security controls is released into the public domain there is a high risk that blaggers and identity criminals will have sufficient information to overcome the security controls in place.

Statement of Truth

I declare that to the best of my knowledge and belief, the information provided in this witness statement is true.

Signature: .... S.P.TSE. Date: 24/10/11.