Document setting out the reasons for granting a Certificate under section 28 of the Data Protection Act 1998

Document: DPA/s.28/MPS/2007/CC2

Bircham Dyson Bell LLP
50 Broadway
London
SW1H 0BL

Tel +44 (0)20 7227 7000

Fax +44 (0)20 7222 3480
DX 2317 Victoria
www.bdb-law.co.uk

TABLE OF CONTENTS

SECTION 28 DATA PROTECTION ACT 1998

1 This Document

1.1 This document sets out the reasons for the Secretary of State for the Home Department ("the Home Secretary") signing the section 28 Certificate under the Data Protection Act 1998 ("the 1998 Act") evidencing the necessity for a national security exemption to the operational units of the Metropolitan Police Service ("MPS") dealing with national security and any the operational units of other police services dealing with national security matters to process personal data derived from the:

1.1.1 London Congestion Charging Cameras (including any extensions); and

1.1.2 Traffic Management Cameras in the Greater London Area (together "the Cameras")

operated by Transport for London ("TfL").

1.2 This Document is referenced as DPA/s.28/MPS/2007/CC2

2 Introduction

2.1 This Document is referred to in the section 28 Certificate ("the Certificate") referred to in paragraph 1.1 above. This Document accompanies the Certificate which is referenced as DPA/s.28/MPS/2007/CC1.

2.2 The Certificate relates to the processing of specific personal data ("the Cameras Data") which comprises the:

2.2.1 images taken by the Cameras ("the Images"); and

2.2.2 personal data (as defined in paragraph 3.2 of this Document) derived from the Images including vehicle registration mark, date, time, place and camera location.

2.3 Before signing the Certificate the Home Secretary considered the following factors:

2.3.1 the functions of police services and their role in the protection of national security;

2.3.2 the creation by all Chief Officers of Police (including the Chief Constable of the British Transport Police) of specialised units to deal with threats to national security including but not limited to the Counter Terrorist Command, Special Branch and the Anti-Terrorist Branch hereinafter referred to as "the National Security Units";

2.3.3 the increased threat to London of a terrorist attack led the Metropolitan Police to seek access to the data derived from the Cameras which were recognised to constitute personal data but which could not lawfully be processed without making use of one or more of the exemptions from the 1998 Act;

2.3.4 the statutory authority under which TfL collects the data from the Cameras and TfL's practice of deleting any personal data that are not required for the purposes of enforcement purposes within a maximum of seven (7) days (twenty-four (24) hours for the Images) of the personal data being collected;

2.3.5 the power of TfL to transfer the Camera Data to the National Security Units;

2.3.6 the specific threat to and the actual attacks on the transport system in London by terrorist activity;

2.3.7 the national security exemptions contained within the 1998 Act and the role of the National Security Appeals Panel of the Information Tribunal ("the Tribunal");

2.3.8 the interaction between police services, the Security Service, the Secret Intelligence Service ("the SIS") and the Government Communications Head Quarters ("GCHQ") (together "the Intelligence Services");

2.3.9 why secrecy is essential to the work of the National Security Units and the damage or potential damage that can be done to national security when secrecy is compromised;

2.3.10 the need to use the "neither confirm nor deny" policy;

2.3.11 the requirements of Human Rights Legislation;

2.3.12 the remedies, other than those under the 1998 Act, open to anyone who wishes to challenge the activities of police officers in respect of harm to them or their property;

2.3.13 the test that should be used to balance the need to safeguard national security and the purposes of the 1998 Act;

2.3.14 that without an exemption under section 28 of the 1998 Act, the 1998 Act would prevent the transfer of the Camera Data to the MPS;

2.3.15 the form and scope of the Certificate;

2.3.16 the checks and procedures included in the Certificate; and

2.3.17 the issues of proportionality in connection with the processing of the Camera Data.

3 The 1998 Act, its national security exemptions and the role of the Tribunal

3.1 The 1998 Act:

3.1.1 came into force on 1 March 2000; and

3.1.2 made new provisions for the regulation of the processing of personal data of living individuals.

3.2 In terms of the 1998 Act, personal data are any data from which the identity of a living individual can be determined, either by themselves or with other data processed by the data controller.

3.3 Personal data can include information such as name and address, email address, telephone number and general contact details and also includes images on film (e.g. CCTV images), photographs and telephone voice recordings.

3.4 In terms of the 1998 Act "processing" means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including:

3.4.1 organisation, adaptation or alteration of the information or data,

3.4.2 retrieval, consultation or use of the information or data,

3.4.3 disclosure of the information or data by transmission, dissemination or otherwise making available, or

3.4.4 alignment, combination, blocking, erasure or destruction of the information or data.

3.5 Section 7 of the 1998 Act created a general entitlement for an individual to ask and be told, by anyone who decided the purposes for which personal data on them are being processed, the following information:

3.5.1 if personal data of which that individual is the data subject, are being processed by or on behalf of that data controller;

3.5.2 a description, in permanent intelligible form, of the personal data that are processed;

3.5.3 the purposes for which those data are processed;

3.5.4 the recipients or classes or recipients to whom those personal data are or may be disclosed;

3.5.5 the source of the personal data; and

3.5.6 the logic involved with any automatic decision making.

3.6 The main rationale for what is known as a "subject access request" is so that the individual data subject can satisfy himself:

3.6.1 as to what, if any, personal data are being processed about them;

3.6.2 that any processing is done for a proper purpose;

3.6.3 that the data are accurate; and

3.6.4 to whom the data may be disclosed.

3.7 If dissatisfied with the outcome of their request the individual can then take corrective action.

3.8 The 1998 Act recognises that there are certain circumstances when it would be inappropriate to comply with specific provisions of the 1998 Act and so provides several exemptions. Section 28 of the 1998 Act exempts personal data from a range of provisions including those of section 7 (subject access requests) if the exemption is required for the purpose of safeguarding national security.

3.9 The requirements of section 28 are set out in the Certificate and are:

3.9.1 By subsection 28(1) of the 1998 Act it is provided that personal data are exempt from any of the provisions of:

3.9.1.1 the data protection principles as set out in Schedule 1 to the 1998 Act;

3.9.1.2 Parts II, III and V of the 1998 Act; and

3.9.1.3 section 55 of the 1998 Act

if the exemption from those provisions is required for the purpose of safeguarding national security.

3.9.2 By subsection 28(2) of the 1998 Act it is provided that a certificate signed by a Minister of the Crown certifying that the exemption from all or any of the provisions mentioned in subsection 28(1) is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact;

3.9.3 By subsection 28(3) it is provided that a certificate under subsection 28(2) of the 1998 Act may identify the personal data to which it applies by means of a general description and may be expressed to have prospective effect.

3.10 The Minister of the Crown specified in section 28(2) must be a member of Her Majesty's Cabinet or the Attorney General.

3.11 It is possible for anyone affected by the Certificate to appeal against the Certificate. The Tribunal can be contacted through the Tribunals Service and further information on the appeal process can be obtained from www.informationtribunal.gov.uk.

3.12 The Tribunal shall consider appeals against the Certificate in accordance with the Information Tribunal (National Security Appeals) Rules 2005. The right to make an appeal is set out in subsection 28(3) of the 1998 Act and the principles that will be used by the Tribunal in determining the appeal are those that used by the High Court of Justice on a judicial review. If the Tribunal determines the Minister did not have reasonable grounds for issuing the Certificate the Tribunal may quash the Certificate.

4 The Functions of the Metropolitan Police and other police services in respect of National Security

4.1 The functions of the Metropolitan Police and the other police services in the United Kingdom are not set down by statute. However, the authority of individual police officers is set out in both statute and common law.

4.2 In respect of national security, the functions of police officers ("the Functions") include:

4.2.1 to assist the Intelligence Services; and

4.2.2 to prevent and detect crime and apprehend and assist in the prosecution of offenders in relation to offences that are connected with national security.

4.3 The Chief Officers of the United Kingdom police services have delegated the day to day management of the Functions to the National Security Units.

4.4 Each police service in the U.K. has its own National Security Unit(s) which work together in respect of the Functions. There is a National Co-ordinator of Counter Terrorist Investigations who is responsible for co-ordinating multi-force investigations. The National Security Units are not statutory bodies and have no legal status. The Chief Officer of each police service is responsible for the personal data processed by the National Security Units, including the Camera Data.

5 Why Secrecy is Essential to the Work of police services in Respect of National Security

5.1 The National Security Units use the same methods of investigation in processing the Camera Data as they do in processing all other data and personal data that comes into their possession.

5.2 Secrecy is essential to enable the National Security Units to carry out the Functions and the activities which are ancillary to the Functions. Examples which demonstrate the need of this secrecy include:

5.2.1 many individuals who cooperate with the National Security Units and the Intelligence Services to carry out the Functions only do so under guarantee of complete confidentiality and anonymity; and

5.2.2 many of the techniques of the National Security Units and the Intelligence Services must remain secret to prevent countermeasures which would disable the effectiveness of those techniques thus damaging national security.

5.3 There are of course numerous specific examples of the need for secrecy which cannot be specified for the reasons set out in paragraph 5.2.2 above.

5.4 The National Security Units and the Intelligence Services work covertly and the effectiveness of those agencies lies in their ability to obtain and provide secret intelligence about matters that others may go to some lengths to keep hidden. It is necessary for there to be an information exchange between the National Security Units and the Intelligence Services.

5.5 It is necessary for the National Security Units to process the Camera Data outside of the restrictions of the 1998 Act due to the history of terrorist threats in and against London and the intelligence that has been gathered in respect of future threats.

5.6 Individuals who are a threat to national security in areas of the UK other than London may operate in London requiring the National Security Units of police services other than the MPS to access the Camera Data for the purposes of safeguarding national security. Such National Security Units will require the same exemptions to the 1998 Act as those National Security Units operated by the MPS.

5.7 To carry out the Functions, the National Security Units must, to the extent permitted in accordance with the statutory and common law authority of the police officers assigned to the National Security Units, process the Camera Data for a wide range of purposes which are covered by the exemption, including but not limited to:

5.7.1 obtaining information from police officers, contacts, the general public and the Intelligence Services;

5.7.2 the monitoring of electromagnetic, acoustic and other emissions, including electronic communications;

5.7.3 the transfer of the Camera Data between the National Security Units of the other United Kingdom police services; and

5.7.4 the disclosure of the Camera Data to the Intelligence Services, Government Departments and Agencies, public authorities, other law enforcement agencies, commercial bodies (e.g. expert advisors and forensic scientists) and other organisations.

5.8 Confirmation of the processing of the Camera Data being processed or release of the Camera Data would reveal the details of how the National Security Units operate and carry on their activities, reducing its effectiveness in the safeguarding of national security.

5.9 If an individual were to become aware that they were subject to the activities of the National Security Units, the Intelligence Services through the National Security Units or the Intelligence Services themselves, they could not only take steps to thwart it but also attempt to discover and perhaps reveal, the methods of operations.

5.10 Compromise of the methods used by the National Security Units and in some cases the individuals involved in particular operations affects all such other operations, as it increases the risks to the police officers deployed and undermines the effectiveness of the operations undertaken.

5.11 Increased knowledge of the methods of investigation deployed by the National Security Units and the Intelligence Services would greatly assist those such as terrorists, spies and serious criminals in planning their activities, so as to reduce the likelihood of detection or interference.

5.12 There are a number of ancillary functions to the operation of the National Security Units, these relate directly to the safeguarding of national security and as with the Intelligence Services, it is necessary for these to fall within the umbrella of secrecy. If outside the umbrella, information about those activities may compromise the Functions and accordingly would damage national security.

5.13 Ultimately, the undermining of the effectiveness of the National Security Units could result in the undermining of the UK police services and a loss of, or a reduction in, the deterrence of those who may be attempting to damage national security. In addition, it could also result in loss of life and the loss of, or a reduction in, the reputation of the National Security Units. This could lead to a reduction in the co-operation required by the National Security Units from individuals and organisations.

5.14 Anything that weakens the effectiveness of the National Security Units weakens the UK's ability to safeguard national security.

6 Transport for London

6.1 The Certificate also confirms that the exemption under section 28 of the 1998 Act applies to TfL.

6.2 Although TfL have the power to transfer the Camera Data to the National Security Units, such power is limited by the operation of the 1998 Act. It is therefore necessary for TfL to be satisfied that the exemption provides that the transfer of the Camera Data to the National Security Units does not breach the 1998 Act.

6.3 TfL shall only transfer the Camera Data to Metropolitan police service Special Branch who shall manage the Camera Data for the purposes of national security. The Commissioner of Police of the Metropolis will be the data controller for the Camera Data following the transfer from TfL.

7 The need and use of the "neither confirm nor deny" policy

7.1 It has been the policy of successive governments neither to confirm nor to deny suggestions put to them on the work of the intelligence and security agencies including the National Security Units. This policy is a way to preserve the secrecy described in paragraph 5 above and entails giving a non-committal answer.

7.2 The need for such a policy and Parliament's acceptance of this is reflected in legislation, including the Official Secrets Acts 1911 to 1989 and the Data Protection Act 1984 the predecessor act to the 1998 Act. The Code of Practice on Access to Government Information, Second Edition 1997, gives "... information whose disclosure would harm national security ..." as a category of information that is exempt from the provisions of the Code. The provisions of the Freedom of Information Act 2000 also consider the need for maintaining the confidentiality of information that would harm national security.

7.3 As far as the law allows, police services apply this policy to the National Security Units and the role of police officers generally in respect of their activities which involve national security, including suggestions of whether a particular individual or group has been under investigation. To ask whether the National Security Units hold personal data on an individual often amounts to asking whether there is or has been an investigation or whether the National Security Units have an interest in that individual or group.

7.4 By logical extension, the policy must apply even if no investigation has taken place. If the National Security Units said when they did not hold information on a particular person, inevitably over time those on whom it did hold information would be able incrementally to deduce that fact, not least because they would not receive the same assurance given to others.

7.5 If individuals intent on damaging national security could confirm that they were not the subjects of the National Security Units interest, then they could undertake their activities with increased confidence and vigour.

7.6 Another complexity would be the handling of cases where the National Security Units have confirmed no interest in an individual or group but subsequently it took an interest as a result of a subject access request. If a change in status had to be notified to the individuals concerned the timing of the change could assist them in their activities. For example, a terrorist may work out what he or she had done at that time to give themselves away. If so, this may allow other individuals to avoid such action in the future, ultimately, this would help them in carrying out their acts of terror.

7.7 Confirmation to individuals that they are subjects of interest, may create or fuel suspicions that associates of theirs are assisting the National Security Units. The consequences of this could be to harm those who are in fact providing the National Security Units with assistance, harm to those wrongly suspected of providing such assistance; and eventually, in either case, harm to the work of the National Security Units and/or the Intelligence Services in that the potential of harm to such persons would act as a strong deterrent to anyone assisting the National Security Units, both in the investigation in question and in any other.

7.8 There are circumstances in which the "neither confirm nor deny" policy is not used. Such a policy is not required when it has been officially confirmed that the National Security Units have undertaken an investigation, e.g. when a prosecution has been made or the National Security Units have confirmed that they are investigating an individual.

8 Safeguards and Statutory Controls

8.1 Due to the covert nature of the investigations by the National Security Units they are intrusive into the privacy of individuals. There are a number of safeguards placed on the National Security Units for these reasons: these include

8.1.1 the Regulation of Investigatory Powers Act 2000 ("RIPA");

8.1.2 the Police and Criminal Evidence Act 1984;

8.1.3 the requirements placed on police officers to obtain the consent of senior police officers and magistrates in specific circumstances;

8.1.4 the National Audit Office;

8.1.5 the internal audit department of each police service; and

8.1.6 the Independent Police Complaints Commission.

8.2 The Chief Officer of each police service must also report to the relevant police authority and the Secretary of State for the Home Department will also take an interest in the activities of each police service and may recommend steps are taken if he believes that there are deficiencies in conduct.

8.3 The Commissioner of Police of the Metropolis must also provide an annual report to the Information Commissioner on the general operation of the Certificate.

8.4 Each police service is subject to the oversight of the independent Interception Commissioner and the Surveillance Commissioner, roles set up by RIPA. The Commissioner sees all information relevant to his functions and can take steps to ensure that the requirements of RIPA are complied with.

8.5 Anyone can make a complaint about a police service:

8.5.1 to that police service;

8.5.2 to the Independent Police Complaints Commission which can be contacted by writing to 90 High Holborn, London WC1V 6BH or via its website at www.ipcc.gov.uk; or

8.5.3 (in respect of matters within its jurisdiction) to the Investigatory Powers Tribunal if they have reason to believe that a Police Force has acted in a way to harm them or their property. The address of the Tribunal is PO Box 33220, London, SW1H 9ZQ.

9 The Test to Balance the need to Safeguard National Security and Data Protection

9.1 Section 28 of the 1998 Act states that "... personal data are exempt ... if the exemption ... is required for the purpose of safeguarding national security". However, the term national security is not defined. Both domestic and European Courts have accepted that the Government has significant discretion in what constitutes national security.

9.2 In addition, when considering safeguarding national security the courts have accepted (Secretary of State for the Home Department v. Rehman [2001] UKHL 47) that it is proper to take a precautionary approach. That is, it is not necessary only to consider circumstances where actual harm has or will occur to national security, but also to consider preventing harm occurring and avoiding the risk of harm occurring.

9.3 The Home Secretary has balanced the need to safeguard national security against the purposes and entitlements conferred by the 1998 Act. The risk to national security through the compromise of the work of the National Security Units and through the National Security Units, and the Intelligence Services, has been covered above. This was balanced against the consequences:

9.3.1 of an individual not knowing whether the National Security Units processes personal data on them arising from a covert investigation;

9.3.2 of an individual not knowing the purpose why it was processed;

9.3.3 of an individual not knowing whether the data are accurate;

9.3.4 of an individual not knowing to whom the data may be disclosed;

9.3.5 for practical purposes, of denying an individual of the opportunity to challenge the:

9.3.5.1 purpose for processing;

9.3.5.2 accuracy of the data processed; and

9.3.5.3 parties to whom the data may be disclosed;

9.3.6 to national security of the individual not correcting inaccurate personal data on him;

9.3.7 of an individual not being able to claim the protection of the non-disclosure provisions; and

9.3.8 of the Information Commissioner or the Courts not having a role in examining the use of the national security exemption in regard to the provisions of the 1998 Act.

9.4 In weighing the factors set out in paragraph 9.3 above, the Home Secretary took account of legal constraints and controls placed on the National Security Units and the requirement to keep the investigations undertaken secret.

10 The Form and Scope of the Certificate

10.1 The Home Secretary has given consideration to the determination of the National Security Appeals Panel of the Information Tribunal in the appeal by Norman Baker MP against the certificates granted to the Intelligence Services when the 1998 Act first came into force.

10.2 The Certificate only relates to the Camera Data as defined in paragraph 2.2.

10.3 As expressly permitted by the 1998 Act, the Certificate identifies specific personal data (the Camera Data).

10.4 The Certificate sets out:

10.4.1 the powers granted by the 1998 Act in respect of exempting data for the purposes of safeguarding national security;

10.4.2 the personal data that are covered by the Certificate;

10.4.3 a summary of the reasons for granting the Certificate;

10.4.4 the notice of the checks and procedures and reporting obligations on the Chief Officer of Police of any police service processing the Camera Data under the Certificate;

10.4.5 the general purposes for which the Camera Data are processed; and

10.4.6 which provisions of the 1998 Act do not apply to the Camera Data in the particular circumstances set out in the Certificate.

10.5 The Certificate applies to processing by both police officers and to civilian support staff assigned to the National Security Units by the Chief Officer of Police.

10.6 The Certificate confirms that the processing undertaken by TfL for the purposes of assisting National Security Units is for the purposes of safeguarding national security. Therefore, TfL is not required to inform any data subjects of the processing it undertakes for the purposes of safeguarding national security.

10.7 Although the personal data covered by the Certificate is specific, the overall scope of the Certificate is general in nature to ensure that an individual certificate is not required for every appeal against the use of the national security exemption for the Camera Data by any National Security Unit. In the vast majority of cases the National Security Units will be using the exemption to preserve the "neither confirm nor deny" policy or to limit the extent of any disclosure.

10.8 The terms of the Certificate were drafted to reflect the functions of the National Security Units and their relationship with the Intelligence Services and the terms of the 1998 Act. A proportionate response was adopted, giving careful consideration to the range of exemptions available and those that were required by the National Security Units for processing the Camera Data in each of the categories specified in the Schedule to the Certificate.

10.9 In particular following the determination of the National Security Appeals Panel of the Information Tribunal in the appeal by Norman Baker MP the "neither confirm nor deny" policy is included within this Certificate, however each subject access request will be considered on its merits and if there is no requirement for the "neither confirm nor deny" policy to be used, e.g. because there has already been a public confirmation that the National Security Units are investigating that individual, the policy will not be used. The exemption contained in the Certificate from section 7(1) of the 1998 Act will not apply to any personal data processed by a police service or TfL if having considered a subject access request the policy of neither confirming nor denying whether Camera Data are held is not required for the purposes of maintaining national security.

10.10 The Certificate does not apply to the processing of the Camera Data for the purposes of the prevention and detection of crime and the apprehension of offenders, if those purposes do not also relate to the safeguarding of national security.

10.11 The Home Secretary made it a condition of the Certificate that:

10.11.1 the Chief Officer of any police service processing the Camera Data must report to the Home Secretary on the operation of the Certificate; and

10.11.2 the Commissioner of Police of the Metropolis is required to provide a report to the Information Commissioner on the general operation of the Certificate.

11 The Checks and Procedures placed on the Metropolitan Police and other police services as a condition of the Certificate

11.1 The Home Secretary considered the requirements in the 1998 Act relating to subject access requests and the internal documents setting out how the Metropolitan Police respond to subject access requests.

11.2 In summary, the obligations require the police service to which a subject access request is made:

11.2.1 to establish if the Camera Data are being processed in respect of that individual;

11.2.2 to decide whether the use of the "neither confirm nor deny" approach is necessary;

11.2.3 if the "neither confirm nor deny" approach is **NOT** necessary, to specify to what extent the national security exemption is still necessary;

11.2.4 to report back to the Home Secretary on the working of these arrangements; and

11.2.5 to report to the Information Commissioner on the general operation of the Certificate.

12 Statutory Power to Transfer the Camera Data

12.1 TfL is responsible for the promotion and maintenance of safe transport facilities and services to from and within Greater London and this power is supported by the further power to do all things which in TfL's opinion are necessary or expedient to facilitate the discharge by it of any of its functions, including the maintaining the safety of the Greater London transport system and services.

12.2 Due to the nature of the threat against the transport system in Greater London from terrorism which can include the threat from numerous extremist groups, the transfer of the Camera Data by TfL to the National Security Units is permitted for the purposes of safeguarding national security

13 Human Rights

13.1 Under Article 8 of Schedule 1 to the Human Rights Act 1998 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, Article 8(2) provides that interference by a public authority is permitted, provided that it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the prevention of disorder or crime.

13.2 The transfer will be necessary for national security, public safety and the prevention of crime as such a transfer will allow the MPS and other police services to use this information for intelligence gathering purposes to safeguard national security and prevent terrorism. The interference to this right must:

13.2.1 correspond to a pressing social need;

13.2.2 be proportionate to the legitimate aim pursued; and

13.2.3 be justified by relevant and sufficient reasons.

13.3 The need to prevent terrorism is a pressing social need.

13.4 The bulk transfer of the Camera Data is proportionate in all of the circumstances, as without all of the Camera Data it is not possible to:

13.4.1 track patterns and eliminate those patterns that are not a threat to national security; or

13.4.2 identify those individuals or groups targeting London using the road network that could pose a threat to national security.

13.5 If only a small proportion of the Camera Data could be held by the MPS, or only vehicles that had been identified by other intelligence means could be targeted, it would not allow the detailed level of analysis required and a threat may not be identified.

13.6 Evidence has been presented to the Home Secretary that the processing of the Camera Data for the purpose of safeguarding national security is required in the interests of national security. The MPS has also established that such a transfer is lawful.

14 General Points

14.1 When reviewing the Certificate the Home Secretary noted that there may be other exemptions under the 1998 Act available in respect of the Camera Data covered by the Certificate.

14.2 The signing of the Certificate does not exclude the possible necessity of signing other national security certificates relating to personal data processed by the Metropolitan Police or other police services.

14.3 The Camera Data shall only be processed for the purposes of processing for matters relating to safeguarding national security, it shall not be used for general policing purposes.

14.4 Access to the Camera Data is restricted to police officers and support staff undertaking work relating to national security purposes.

15 Conclusion

15.1 Having considered the factors above, the Home Secretary decided it was proper for him to sign the Certificate in relation to the exemption of the processing by the Metropolitan Police, other police services and TfL in respect of the Camera Data.