



Date: 18 December 2013

Item: 15 Personal Data Disclosure to the Police and Other Law Enforcement Agencies

This paper will be considered in public

1 Summary

1.1 This paper provides an update to the Committee on the operation of TfL's disclosure of personal data policy to the police and other statutory law enforcement agencies.

2 Recommendation

2.1 **The Committee is asked to note the report.**

3 Background

3.1 The policy on the disclosure of personal data to the police and other law enforcement agencies was approved by the Board on 7 December 2006. The Board asked for a high level report on the operation of the policy to be provided to the Audit and Assurance Committee on an annual basis.

3.2 TfL holds a range of information about its customers and employees and in disclosing personal details to the police and other statutory law enforcement bodies without the subject's consent, exercises the exemption under section 29 of the Data Protection Act (DPA) 1998, for the purposes of crime prevention and detection purposes.

3.3 TfL receives detailed requests from the police and other law enforcement bodies¹ for the disclosure of personal information on customers and TfL employees. In accordance with the agreed policy, TfL considers all such requests on a case by case basis and releases personal data where it is lawful to do so and is consistent with its powers. This paper provides the Committee with a summary picture of the data disclosed this year.

4 Operation of the Policy

4.1 Information Governance (IG) in General Counsel advises on the implementation of the policy and assesses compliance with current legislation and best practice.

4.2 The operation of the policy in the context of the day to day processes, procedures and auditing of disclosures to the police continues to be managed by the Crime and Antisocial Behaviour Investigation Team (CIT) within TfL's new Directorate of

¹ Includes national security and other agencies with a statutory role in crime prevention and detection.

Enforcement and On-street Operations² (EOS) in Surface Transport. This team deals with requests for personal data made to TfL by the police and other Statutory Law Enforcement Agencies (SLEAs) with the following exceptions:

- a) police requests for access to information, including CCTV images, held by London Underground Limited (LUL). These requests are processed directly by LUL, or in the case of CCTV requests the British Transport Police (BTP) on its behalf;
- b) police requests for information on licensed drivers, held by the London Taxi and Private Hire, for example for investigating allegations of sexual offences and other serious crimes. These requests are processed directly by London Taxi and Private Hire; and
- c) Victoria Coach Station, Bus operations, Road Network Compliance and London River Services may also respond directly to the police and law enforcement agencies for requests, primarily for CCTV they hold. All departments follow TfL's policy and procedures and are trained and audited by EOS, overseen by IG.

4.3 Since May 2012, EOS has also taken responsibility for responding directly to requests from non-police bodies that have a statutory role in crime prevention and detection (for example, the Vehicle and Operator Services Agency (VOSA), local authorities, HM Revenue & Customs, the National Crime Agency).

5 Overview of Requests and Disclosures

5.1 Figure 1 shows the volume of all police and SLEA data requests made to EOS since 2007 (for full year January - December) and year to date for 2013 up to 31 October 2013. To the end of October this year, 8,289 data requests have been made to EOS. The forecast for the full year for 2013 is estimated at 9,800, this equates to nearly a 30 per cent increase on the average of the last three years. Over the same period crime on London's transport network has reduced by over 30 per cent. The increase reflects a number of factors including the higher awareness of the type of data available within TfL, more thorough investigations of bus crime and improved back office systems and through this the quality of data.

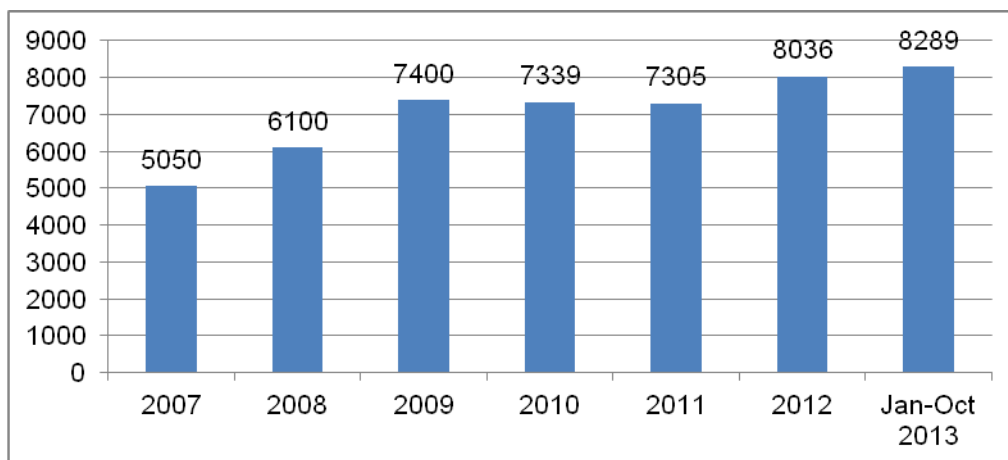


Figure 1: Breakdown of request (by volume) from Jan – Dec 2007 – Oct 2013

² The Enforcement and On-street Operations Directorate has recently replaced the Community Safety, Enforcement and Policing Directorate and incorporates new enforcement functions and responsibilities that previously sat with other areas of Surface Transport.

5.2 The Metropolitan Police Service (MPS) account for the majority of requests made to EOS. Figure 2 shows a breakdown of data requests by requesting agency (by percentage) from 1 January to 31 October 2013.

SLEA	No of requests	Percentage
MPS	7,250	87
BTP	506	6
Other police forces	165	2
National Security	254	3
Non-police bodies that have a statutory role in crime prevention and detection	88	1
City of London Police	26	<1

Figure 2: Data requests by requesting agency

5.3 Figure 3 shows data requests by crime/incident type year to date. Requests fewer than 100 in number are not shown.

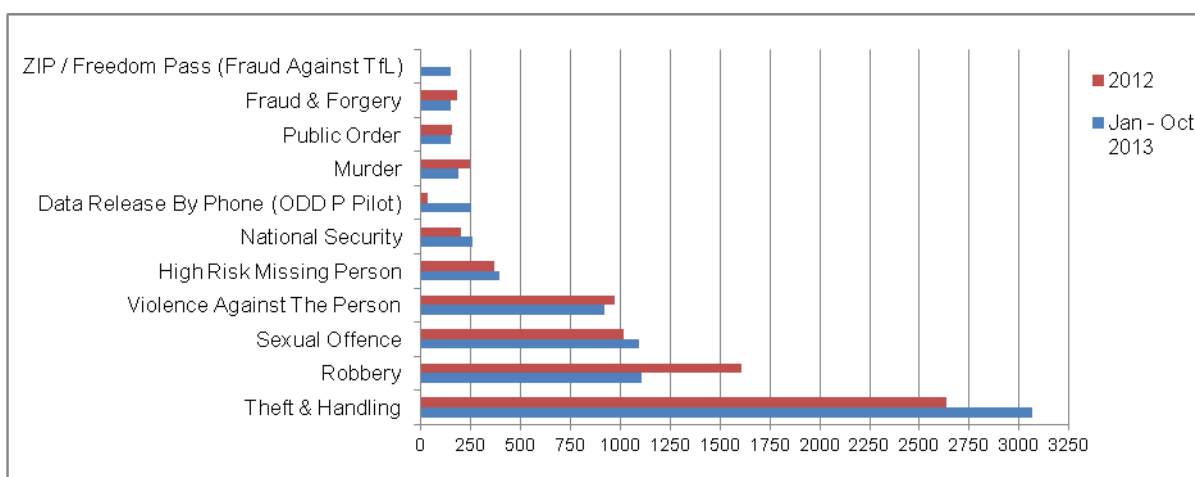


Figure 3: Data request by crime type

6 Overview of Requests and Improvements

6.1 EOS continually reviews how best to manage current and projected levels of demand. Guidance to the police and SLEAs has been issued and is routinely updated and placed on their intranet sources.

6.2 The purpose of this guidance is to provide clear advice on how data requests should be made and how they will be managed once received by TfL. This guidance assists EOS provides a uniform and structured approach in accordance with the TfL policy and ensures that any disclosures are lawful, necessary and proportionate. Requests are dealt with on a case by case basis, but in order to manage demand are triaged when they are received, determining if and how they will be dealt with.

6.3 As a result of these changes and EOS' close working with the Police, EOS has seen an increase in the accuracy of submission and consequent reduction in

rejected cases. This has been matched by a small increase in the proportion of requests which result in TfL making a disclosure (see Figure 4).

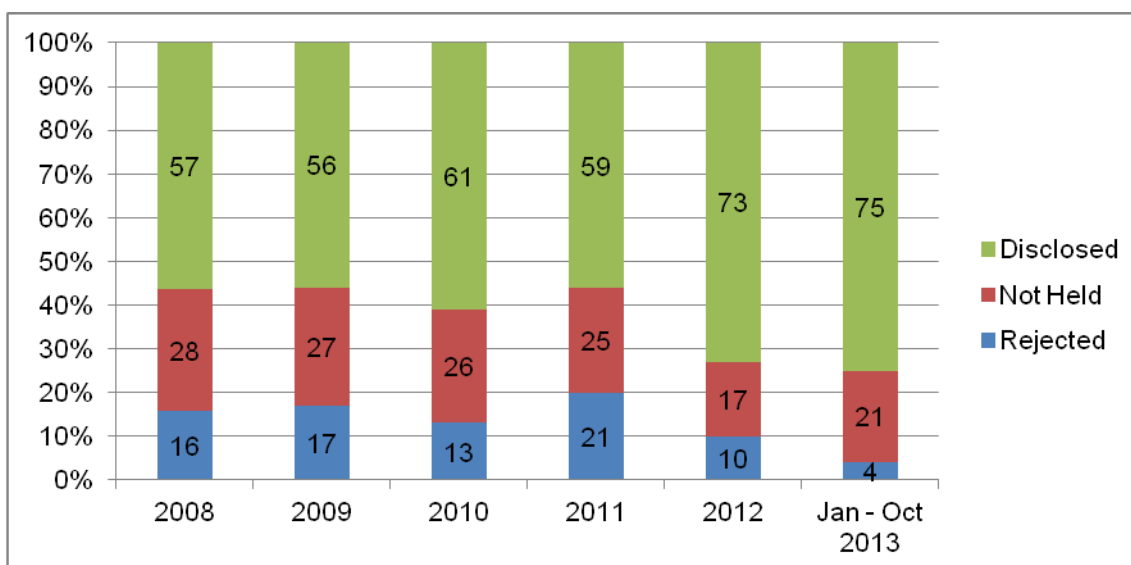


Figure 4: Breakdown of responses to data requests - Data Disclosed, Not Held or Rejected

- 6.4 Only four per cent of requests were rejected this year. The option is always open for the police to request a court Production Order via the Crown Court to obtain the data in instances where TfL has refused, with legitimate reason, to disclose data. The main reason for such rejections has to do with the proportionality of the data requested. In 2013, there were a total of 11 Production Orders received by TfL.
- 6.5 As part of the process reviews, improvements have also been made in the time taken for disclosures. The speed of data disclosure can be vital to police investigations and swiftly bringing offenders to justice, preventing further crimes being committed by that offender against our staff, passengers or infrastructure.
- 6.6 The average time taken for a request to be disclosed in 2011 was 7.5 days, in 2012 this decreased to 4.8 days, and this year to date the average stands at 2.8 days. By nature, some requests will take time as they are complex and can take further liaison with officers to ensure that only data which is necessary to the investigation is released.
- 6.7 In 2011, 44 per cent of requests were turned around within one day of receipt, in 2012 this rate stood at over 52 per cent, this year to date it stands at 63 per cent.
- 6.8 Data disclosures by the team in EOS and elsewhere are regularly audited internally to ensure that all work is carried out in accordance with TfL policy and the principles of the Data Protection Act 1998.
- 6.9 Overarching 'Information Sharing Protocols' (and a number of subsidiary procedures) with the MPS, City of London Police (CoLP) and the BTP have been concluded and implemented. A similar agreement has been finalised with the National Crime Agency. These agreements streamline the process for entering into arrangements for the regular sharing of information with the police while ensuring that all relevant legal and operational requirements are satisfied.

- 6.10 TfL continues the bulk transfer of data (but not images) collected by Road User Charging and traffic management Automatic Number Plate Recognition (ANPR) cameras to the MPS for the purpose of safeguarding national security. The Home Secretary has certified that it is necessary that this transfer (and the associated processing of this data by the MPS, other police forces and national security agencies) be exempted from a number of provisions of the DPA, in order to safeguard national security.
- 6.11 The Mayor's manifesto commitment to make data collected by Road User Charging ANPR cameras available to the MPS for use in crime prevention and detection (in addition to its existing use for national security purposes) is currently being progressed, in conjunction with the MPS, Mayor's Office for Policing and Crime and the GLA. It is hoped that this will result in their ability to share these cameras and use this data from mid-2014.

7 Conclusion

- 7.1 The fact that data requests and disclosures continue to increase demonstrates the value of the data to the police and other SLEAs for the investigation, prevention and detection of crime on the TfL network and threats to national security. As a result of this work, TfL is making a prominent contribution to the safety and security of London's transport infrastructure and its passengers by enabling Police partners to access data they consider to be necessary to their efforts and contributing to the reductions in crime seen on the transport system over the past few years.

List of Appendices to this report:

A paper on Part 2 of the agenda contains exempt supplemental information

List of Background Papers:

None

Contact: Steve Burton, Director of Enforcement and On-street Operations
Number: 020 3054 0755
Email: steve.burton@tfl.gov.uk