IN THE FIRST-TIER TRIBUNAL **Case No.** EA/2012/0127
GENERAL REGULATORY CHAMBER
INFORMATION RIGHTS

ON APPEAL FROM:

The Information Commissioner's
Decision Notice dated 21st May 2012
FS50421919

Appellant: **Transport for London**

Respondent: **Information Commissioner**

Heard at Field House London on 22nd and 23rd January 2013

Date of decision: **28 February 2013**

Before
John Angel
(Judge)
and
Dr Henry Fitzhugh and Michael Jones

Attendances:

For the Appellant: Robin Hopkins
For the Respondent: Edward Capewell

Subject matter: s.24(1) national security
Cases: *London Borough of Camden v The Information Commissioner &YV* [2012] UKUT 190 (AAC)
Secretary of State for the Home Department v Rehman [2001] UKHL 47; [2003] 1 AC 153
Quayum (on behalf of the Camden Community Law Centre) v IC and FCO [2012] 1 Info LR 332
MB v Secretary of State for the Home Department [2007] UKHL 46, [2008] 1 AC 440

Decision

The appeal is allowed.

Reasons for Decision

Background

1. This appeal concerns information relating to speed limits on London Underground's Victoria Line which is part of Transport for London ("TfL").

2. TfL uses a 'simulator' for emergency planning, which is a computer platform that models capability for controlling services on the London Underground. It is based on a great deal of data about London Underground lines, stations and trains.

3. Some of this data (for example train timetables and an approximation of live day-to-day train movements) is actively placed in the public domain, for the convenience of passengers and for transparency and monitoring purposes. Other inputs for the simulator are not actively publicised, but they cannot really be concealed: London Underground is an 'open access' transport system (i.e. unlike an airport, you can enter and move around on the Underground without having your identity or purposes checked), meaning that a lot of detail about the system is readily observable. Train enthusiasts in particular gather and share a great deal of information about the London Underground. Some other inputs for the simulator are not placed in the public domain, nor are they readily observable – for example because they are very technical, or because they do not arise under everyday conditions.

4. This case is about information in this last category.

The Request

5. The original request was made by the requester by email dated 4th April 2011. In that email he wrote in part:

> *"Please provide me with details of the line speed limits on the Victoria Line between stations and permanent speed restrictions imposed by track circuit name.*
> *…*
> *I would also like to know the speed limits of the various sidings, crossovers and the Northumberland Park depot approaches…"*

6. After some intermediate correspondence TfL's substantive response to the information request was provided by email dated 13th August 2011. In it, TfL confirmed that the information requested was held, but was being withheld on the basis of section 38 FOIA (health and safety). The response stated, so far as here relevant:

> *In this instance the exemption has been applied as disclosing detailed operational information and train movement data could be of benefit to those who wish to act maliciously…the type of information you have requested could be used to build up a picture of our operational services, identify pinch points and allow individuals to identify locations to disrupt services or commit malicious acts…*

7. On 17th August 2011 the requester asked for an internal review. After some chasing TfL provided a substantive response on 19th October 2011. In that response they relied for the first time on section 24 FOIA. Further information on the application of the exemptions was provided to the requester by email dated 29th November 2011.

8. The requester made it known that he wanted that information in order to improve the accuracy of his own simulator, a computer product made and marketed for train enthusiasts to participate in 'role play', i.e. to pretend they are in charge of a London Underground control room. The requester is (or at the time of the request, was) involved with a business called Simsig, which advertises itself as for "armchair signallers". The following passage is an extract from its website (with emphasis added):

> *"SimSig places you in the signaller's seat and lets you control the trains. You will be presented with an environment closely resembling a real signalling control centre, including the screen display and controls. It recreates the signalling as realistically as possible and it is up to you to route the trains to their destination and do your best to keep them on time. You will have to make the same kind of decisions that real signallers do to keep the railway running as smoothly as possible.*
>
> *Sounds easy, doesn't it? Well, it is ... until something goes wrong. Can you cope with the everyday challenges of late running trains, random delays, signal and point failures, engineering works, or bad weather?"*[1]

Complaint to the Commissioner

9. The requester made a complaint to the Commissioner pursuant to section 50 FOIA on 21st October 2011. Thereafter the Commissioner carried out his investigation in the usual way. TfL's detailed explanation of why it sought to rely upon sections 24 and 38 was contained in a letter to the Commissioner dated 2nd March 2012.

10. The Commissioner issued a decision notice dated 21st May 2012. His main findings were as follows:

[1] See www.simsig.co.uk.

a. In respect of section 38, he accepted that the safety of individuals would be endangered where disclosure would encourage an attack on London Underground. However he concluded that the exemption was not engaged as TfL had failed to demonstrate a causal link between disclosure of the requested information and endangerment and that therefore there was no need to consider the public interest test ("PIT");

b. The Commissioner also found that the national security exemption (section 24) was not engaged. This was on the basis that as TfL's arguments relating to the engagement of both exemptions were largely the same; it followed that the Commissioner could also conclude that the section 24 exemption was not engaged.

Appeal to the Tribunal

11. TfL appealed to the First-tier Tribunal ("FTT") by notice of appeal dated 18th June 2012 on the grounds that both exemptions were engaged and that the public interest balance favoured maintaining both exemptions.

12. The case was heard over two days and TfL called three witnesses:

a. Kevin Paul Clack is the Acting Network Security Manager for London Underground Ltd ("LU"), which is a subsidiary of TfL. He has held this position since April 2012 and is responsible for co-ordinating LU's approach to security risks. Previously he held the Deputy Network Security Manager role for 14 years;
b. Charles Andrew Apostole was at the time of the request the Service Control Manager for the Victoria Line of TfL. He ran the Victoria Line Service Control Centre, and managed the staff employed there and had landlord responsibility for the premises. He has now moved on to another position;
c. Adrian Stephen Dwyer is the Counter-Terrorism Adviser of British Transport Police. He examines terrorist methodology and the appropriateness and applicability of countermeasures.

13. Mr Clack and Mr Apostole both gave evidence in closed sessions as well as in open court.

14. There was an application under rule 14 of the Rules of Procedure in relation to Mr Clack's originally lodged closed witness statement. As a result some of the closed evidence subsequently became open.

Legal framework

15. The qualified exemption at section 24(1) of FOIA provides that:

> *(1) Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security.*

16. Although we are not bound by other decisions of the FTT: see *London Borough of Camden v The Information Commissioner &YV* [2012] UKUT 190 (AAC) §12 "previous decisions are of persuasive authority and the tribunal is right to value consistency in decision-making. However, there are dangers in paying too close a regard to previous decisions. It can elevate issues of fact into issues of law or principle". With this in mind we refer to decisions of the FTT which the parties have brought to our attention as well as decisions of higher courts by which we are bound.

17. The requisite threat to national security need not be direct or immediate in order for section 24(1) to be engaged: see *Kalman v IC and Department for Transport* [2011] 1 Info LR 664 at §34 and also for example *Summers v IC and Commissioner of Police for the Metropolis* (EA/2011/0186) at §8, both of which base that position on the approach of the House of Lords in *Secretary of State for the Home Department v Rehman* [2001] UKHL 47; [2003] 1 AC 153, and in particular the following extract from the speech of Lord Slynn at 182C-F:

> *"The sophistication of means available, the speed of movement of persons and goods, the speed of modern communication, are all factors which may have to be taken into account in deciding whether there is a real possibility that the national security of the United Kingdom may immediately or subsequently be put at risk by the actions of others. To require the matters in question to be capable of resulting "directly" in a threat to national security limits too tightly the discretion of the executive in deciding how the interests of the state, including not merely military defence but democracy, the legal and constitutional systems of the state, need to be protected. I accept that there must be a real possibility of an adverse affect on the United Kingdom for what is done by the individual under inquiry but I do not accept that it has to be direct or immediate."*

18. According to other Tribunals it is not sufficient for information merely to relate to national security; rather, the exemption must be "required" for the purposes of national security. "Required" here should be interpreted as meaning "reasonably necessary": *Kalman* at §33.

19. TfL brought to our attention the view expressed by the Tribunal in *Quayum (on behalf of the Camden Community Law Centre) v IC and FCO* (EA/2011/0167), [2012] 1 Info LR 332 at §43:

> *"… national security is predominantly the responsibility of the government and its various departments. The Second Respondent has contended, correctly in the Tribunal's view, that the Tribunal must at least initially afford due weight to what is regarded as the considered view of such departments, even though the exemption entails an element of public interest and the balancing test. In particular, and again the Tribunal endorses this approach, particular weight should be afforded to the views of the government*

or its appropriate department with regard to its or their assessment of what is required to safeguard national security in any given case and the prejudice likely to result from disclosure."

TfL argue that the Tribunal need not 'defer' to expert or experienced witnesses. It should, however, afford their evidence due weight, particularly on technical matters (such as simulators and train movements as explained by Messrs Clack and Apostole in evidence) and on security matters (provided in evidence by Messrs Clack and Dwyer). We have some sympathy with this argument.

20. The Commissioner also drew the Tribunal's attention to certain dicta of Baroness Hale of Richmond in the case of *MB v Secretary of State for the Home Department* [2007] UKHL 46, [2008] 1 AC 440, a case concerned with disclosure in the context of control order proceedings. Sounding a note of caution as to Executive reliance on matters of national security her Ladyship stated at [66] and [72]:

> *Both judge and special advocates will have to probe the claim that the closed material should remain closed with great care and considerable scepticism. There is ample evidence from elsewhere of a tendency to over-claim the need for secrecy in terrorism cases: see* Turner & Schulhofer, The Secrecy Problem in Terrorism Trials *(2005), Brennan Centre for Justice at NYU School of Law. Both judge and special advocates will have stringently to test the material which remains closed…*
> *…*
> *Where the court does not give the Secretary of State permission to withhold closed material, she has a choice. She may decide that, after all, it can safely be disclosed (experience elsewhere in the world has been that, if pushed, the authorities discover that more can be disclosed than they first thought possible)…*
>
> Emphasis added.

21. Section 38(1)(b) of FOIA provides that:

> *(1) Information is exempt information if its disclosure under this Act would, or would be likely to—*
> *...*
> *(b) endanger the safety of any individual.*

22. The threshold relied upon by TfL in this case is "would be likely to" rather than "would". The individuals concerned are those using and working on the London Underground (in particular, the Victoria Line).

23. "Endanger" for the purposes of section 38 has been held to have the same meaning as "prejudice": *PETA v IC and University of Oxford* [2011] 1 Info

LR 906 at §§29-30. Other Tribunals have taken a different view. In *BUAV v IC and Newcastle University* (EA/2010/0064), the University argued for the "prejudice" interpretation while BUAV argued for a higher threshold of a "weighty chance" of a risk arising. At §18, the Tribunal said this:

> *"We do not fully accept either submission. We must take into account that in s. 38(1) Parliament chose to use the word "endanger" and did not refer either to "injury" or to "prejudice". On the other hand, considering the statutory purpose of freedom of information, balanced by exemptions, we are not persuaded that it would be right to read the word "endanger" in a sense which would engage the exception merely because of a risk. A risk is not the same as a specific danger. Every time a motorist drives on the road there is a risk that an accident may occur, but driving is only dangerous when a particularly risky situation arises. So, for example, there is always a risk that a researcher might become a target for persons opposing animal research by unlawful and violent means, but the researcher's physical health would not be endangered unless a specific attack were made. We need to consider the likelihood of such an attack, and the likelihood of other conduct which would endanger mental health or other aspects of safety."*

How London Underground works

24. Mr Apostole gave detailed evidence to us on how London Underground, particularly the Victoria Line, works. We set down what he said below.

25. The disputed information consists of the theoretical maximum speed permitted on each part of Victoria Line track, taking into account factors that would make it unsafe to exceed that speed, e.g. curves in the route, track junctions and so on. In practice, for many areas of track, trains will rarely be travelling at this maximum. They will regularly need to accelerate and decelerate in order to keep a safe distance from other trains, to ensure they are able to stop at platforms, to keep to timetables and so on.

26. London's Metro system comprises the London Underground Heavy Rail Network and the Docklands Light Railway. It is the largest such network (by route miles) in the world. It consists of 311 stations, and about 271 miles of track over 11 lines, of which just under half is underground. In 2011, the system carried a daily average of about 3.2 million passengers.

27. The Victoria line, which forms part of the London Underground system, is just over 13 miles long. It has 16 stations, of which 15 have interchanges with other Underground, Overground or National Rail stations. Unlike a number of other London Underground lines, the whole of the Victoria Line's passenger line is below ground. The connection to the Northumberland Park depot, where fleet maintenance work is carried out, is however above ground.

28. In 2011 the Victoria line carried a daily average of about 600,000 passengers. During peak hours each train carries an average of well over 800 passengers. The journey from the southern end of the Victoria line at Brixton to its northern end at Walthamstow takes 32 minutes. In normal circumstances, the average maximum speed reached by a Victoria Line train is about 50 mph. Trains run approximately every two minutes during peak periods in each direction.

29. Trains on the Victoria line are automatically operated. Each train has a train operator (driver), but once the train operator has closed the train doors and pressed the start buttons, the trains run automatically to the next station, at speeds dictated by the complex (and recently changed) system of codes and limits.

30. The Victoria Line has recently gone through an upgrade, which included a new signalling system, a new Service Control Centre and a new fleet of trains which have increased the capacity of the line. The interaction between the concept of speed limits and the way trains run is fairly complex.

31. The codes were transmitted to the trains by pulses in its electric current. These codes were fed into the train by 'pick up coils' located in front of the leading wheel of the train and fed to the safety box.

32. The new system works differently. It does not use the code system just described

33. Instead, trains are built and programmed so that they automatically move at speed up to their 'limit of movement authority'. This is different from the speed *limit* at which trains are physically and safely capable of travelling. The limit of movement authority is a centrally-determined limit set *within* the physical speed limit for the track. It is generated by the train's on-board signalling system, which looks ahead to the position of the train in front and sets a target speed for the train to run at by reference to the distance to the next block stopping point (i.e. either the next signal or the next block marker board).

34. There was also a transition period in place between the old and new systems while the upgrade work was being done. This transition period began in approximately October 2009 and ended in approximately March 2011. This enabled the line to operate with a mixed fleet of old (1967) and new trains.

35. Once the last 1967 stock train had left the line for good, the process of removing the old assets redundant signalling equipment and commissioning the new assets commenced. The removal of the old assets was carried out over a series of weekend closures, with the final part of the line being completed in May 2012.

36. The above explanation is about the speeds at which trains actually move on the Victoria Line under normal conditions. This sort of information can be explained publicly without causing any problems: it is closely connected with the actual journey time and timetabling information such as that published on 'Trackernet', a system by which information feeds are made available to software application developers whose products enable members of the public to plan their journeys and so on.

37. Speed limit information, however, is not in the public domain. It is closely connected not with train operations in normal conditions, but with what can be done with trains under much more unusual conditions, as arise in emergency situations.

38. Speed restrictions on the Victoria Line fall into two categories. First, 'maximum safe speed' is the term used for the fastest speed at which, in normal conditions, a train can travel in a way that achieves optimal journey efficiency within safety bounds. This speed is variable but has an upper limit of 50 mph on the Victoria Line. This applies to all points on the Victoria Line where an unimpeded run is envisaged. Normally, all trains will travel up to the full line speed of 50 mph subject to the position of the train ahead.

39. The disputed information in this case is about the second type of speed restriction, namely 'permanent speed restrictions'. These vary across the Line due to track curvature, intersections and crossovers between lines and so on. A permanent speed restriction is always lower than the maximum safe speed and is applied to a specific area where a track or other physical constraint requires a lower speed. This is dictated by the specific safety implications for each particular part of the Line. Strictly speaking (contrary to the wording of the request), permanent speed restrictions do not relate to specific track circuits, but rather to allocated nodes, a node being a fixed point where data can enter a system. Generally a node does line up with a track circuit boundary, but this is not necessarily the case. The disputed information consists of the permanent speed restrictions by node. It would not be possible to determine this information for track circuits as such, but in Mr Apostole's opinion very little turns on that. The disputed information is for all intents and purposes the information the requester is asking for.

40. As mentioned earlier Victoria Line trains are not normally driven by the train operator as such, but are automatically controlled. Also trains can be driven manually in certain conditions such as failure or under certain emergency conditions. In most cases, the speed limit for manual driving is 10 mph.

Use of simulators

41. Mr Apostole informed us that the Service Control Centre for the Victoria Line contains a Windows-based computer system which tracks and

displays exactly where all trains are on the line in real time. A replica of this system is also used, known as a simulator, which does the same thing but using hypothetical inputs which can be manipulated and varied for training and planning purposes, for replaying incidents (as a learning exercise) and for testing new timetables and software updates prior to their being introduced on to the live signalling system. It is a very important tool for emergency planning. TfL can create any number of different scenarios on the simulator and then determine the optimal way to move trains in response to that scenario.

42. For obvious reasons, the simulator used needs to be accurate, i.e. to allow for accurate modelling of exactly how trains can be moved in response to an emergency, how long it would take to move them and so on. This accuracy requires a full set of correct technical information. Permanent speed restriction data is one category of input necessary for an accurate simulator. Many other categories of necessary input are publicly available, such as train timetable information, distances between stations, number of carriages per train and so on.

43. TfL simulators are developed by commercial IT providers for its internal use only. Mr Apostole informed us, however, that private individuals and companies develop their own simulators for sale, including online, to rail enthusiasts who can use these simulators for role-playing, i.e. to get a feel for the role and work of a signal operator. Because, to the best of Mr Apostole's knowledge, they use only publicly available information, they cannot, in his view, be used for accurate modelling of how trains are likely to be moved in response to emergency incidents.

44. Mr Apostole says that if the disputed information became publicly available, it together with a couple more types of information would supply the missing ingredients which would allow a simulator to replicate the accuracy and sophistication of the simulator TfL uses to plan its responses to emergency situations. Mr Apostole also says that the requester's intention is to do exactly that and that TfL's concern is with the harm that could be done with this simulator by less innocent parties.

45. The disputed information is innocuous when considered in isolation, but in Mr Apostole's view it is an essential component for building a 'simulator', i.e. an accurate computer model allowing for predictions as to exactly how London Underground trains can move and – importantly for this case – how they would be moved in response to an attack or security incident.

46. While such a simulator would not be harmful in innocent hands, it would be, in the view of all the witnesses, very helpful to those who wish to plan attacks on the Victoria Line. The concern is not so much that the public availability of a simulator would lead to an attack. The concern is more that a simulator would allow the attacker to maximise the harm from an attack, by using accurate predictions of exactly where and how trains would be moved in response to the incident. Simulators could be used to undermine the speed and effectiveness of London Underground's response to an

attack. This could also make a plan more attractive (and thus more likely to be acted upon) to an attacker intent on maximising harm. In that sense, the witnesses inform us, disclosure could – because of its value in building an accurate simulator and its effect of increasing the confidence of a terrorist – increase the likelihood of an attack.

47. The simulator is used for training purposes. It is also used for planning in detail TfL's responses to emergency situations. TfL can test any number of scenarios: for example, positioning all trains where they would be in a normal rush hour situation, and then simulating incidents at points X, Y and Z on the line simultaneously, at two-minute intervals or whatever the case may be. The simulator helps TfL to plan how it should move trains for an optimal response to that emergency. TfL has declined to allow the simulator packages to be replicated and exploited for commercial gain by its IT provider, for security reasons.

48. Mr Apostole informs us that a 'rough and ready' replica of the simulator could be built using publicly available data, such as data about journey times. This would be a piece of software modelling how the Victoria Line operates. A simulator based only on publicly available information such as Trackernet data would only model how trains are likely to move under *normal* conditions. Trackernet data does not allow for the simulation of likely train movements in emergency conditions. More detailed, technical and unavailable internal data is needed in order to build a simulator capable of accurately modelling emergency scenarios. One necessary set of inputs for doing so consists of details of line speeds on different stretches of track – i.e. the disputed information in this case.

49. In Mr Clack's view a simulator which allows for accurate modelling of emergency situations would enable a potential attacker to plan an attack in a way that maximised harm. The attacker could calculate from which parts of the network trains would be slowest to escape, or find it most difficult to escape, and plan their attacks accordingly. They could predict that following an incident at a point X at a certain time, trains would be moved so as to reach point Y at exactly such-and-such times. They could then co-ordinate and time their attacks accordingly.

50. Again in his view these examples illustrate how an accurate simulator can be used to plan attacks in a way that does most damage and which makes evacuation most difficult (or even counter-productive) and frustrates the swift access of emergency services. Given that terrorists generally seek to mount attacks which do as much damage as possible, there is also a real possibility that the availability of an accurate simulator causes a would-be attacker to make plans which seem much more attractive and therefore more likely to be acted upon. In his view, all of this constitutes a serious health and safety risk and, given the national importance of London Underground (including its economic importance), a national security threat.

51. Mr Clack considers that this risk is very real and that it is far from remote, hypothetical or speculative. He is aware that the motivation for this request is to build a more accurate simulator, which is sold commercially, as a hobby item for train enthusiasts. In his view the disclosure of the requested information would result in (or at least make a significant contribution towards) an accurate simulator which uses track speed limit data to allow for the modelling of emergency situations being made available for purchase or use by someone who did wish to do harm to the London Underground.

52. The closed evidence given showed how an accurate simulator could be used to plan and execute an attack on the Victoria Line in a way that maximised the damage caused. This was done by reference to a series of pictures taken from TfL's simulator. The evidence is convincing.

Importance and vulnerability of London Underground

53. Mr Clack considers that London Underground is possibly the most important component of the capital's transport infrastructure. To take one example, Victoria Underground station can have over 82 million people enter and exit in a year, with millions more using it to change between lines. To put this in perspective, this exceeds the annual number of people travelling through Heathrow airport, which he understands to have reached around 69 million people. In other words London Underground is of enormous importance to the economy of London.

54. Mr Clack also gave us the following evidence. The UK Government has expressly recognised that London Underground needs to be able to run services even during sustained periods of heightened threat, to resume services as soon as possible after a security incident and to ensure the continuing confidence of users in its safety and security. The Government, through the Department for Transport, issues legally binding instructions under section 119 of the Railways Act 1993 which mandate minimum standards for security and related matters aimed at reducing the risks and impact of terrorist acts. These instructions were first issued in 2003 and are due to be updated imminently.

55. The *National Risk Register of Civil Emergencies*, published by the Cabinet Office, recognises attacks on transport infrastructure as a category of national security risk. It also includes the potential for non-conventional attacks such as the release of a chemical substance.

56. Mr Clack draws the above points to the Tribunal's attention to illustrate that London Underground is of *national* as well as metropolitan importance.

57. He informs us that the London Underground system is a major potential target for terrorist attacks. This has been the case for significant periods of its nearly 150-year history, with the risks of such attacks increasing in recent years. The world famous London Underground brand, coupled with

the global prominence of London, makes it an attractive target for those seeking maximum publicity for attacks which could kill or injure a great number of people.

58. In Mr Clack's view the prospect of an attack on London Underground is far from theoretical or remote. The 1970s and 1990s saw the Underground targeted on several occasions by Irish Republican terrorists. In 2005, three terrorists and 39 other people were killed in bomb attacks on three different London Underground trains. Several hundred more people suffered serious injuries. Two weeks later a further group attempted similar attacks, but were unsuccessful due to their devices malfunctioning.

59. Other mass transit railway systems around the world have also been subject to terrorist or malicious attacks which have produced fatalities and/or injuries: for example in 1995 there was a poison gas attack on the Tokyo subway, in 1995 and 1996 there were bomb attacks on the Paris Metro, in 2003 there was an arson attack on the metropolitan railway in Daegu, South Korea, in 2004 there were coordinated bomb attacks on the Madrid suburban rail system, and in 2004 and 2010 there were bomb attacks on the Moscow underground.

60. Mr Dwyer of the British Transport Police supports TfL's view of the seriousness of the risk of an attack on London Underground. He draws our attention to the a number of open-source documents which address the issues of threat and risk in detail: *House of Commons Transport Committee* report HC191, published in 2008 (particularly pages EV4 and EV125); the *Intelligence and Security Committee Report into the London Terrorist Attacks on 7 July 2005* Cm 6785 (see page 31, paragraph 113); *Security risk assessments in public transport networks (DOI: 10.1243/09544097JRRT409) - Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit 2011 225: 417*, by M M Sánchez; *Amendments to the Anti- Terrorism Crime and Security Act 2001*, published in 2011 (page 8).

<u>London Underground's security strategy and its limits</u>

61. Mr Clack informed us that London Underground adopts a range of methods for reducing the risk of such attacks. These include: regular security checks by station staff to provide a visible deterrent and to identify any suspicious items or behaviour; management of litter bins and bulk storage facilities to reduce the opportunity for concealment; high standards of lighting and CCTV to increase surveillance; management of the security between public and non-public areas; management of visitors other than customers to ensure they have a bona fide reason to be present; vigilant staff who know how to report concerns to police; measures to encourage security awareness of customers and robust - often detailed - emergency response plans.

62. Mr Clack explained that the concern in this particular case is with this last aspect of the security strategy in particular. Emergency response plans extend beyond TfL itself. Common response plans have been developed across TfL, the emergency services and other agencies. There are special arrangements in place with the emergency services (including specially trained personnel, personal protective equipment and detection capability for non-conventional attacks). The British Transport Police have specialist units to respond to potential or actual terrorist incidents.

63. Notwithstanding this evolving security approach, the risk of an attack can only be reduced, not eliminated. There are a number of features of London Underground which mean that there is always a level of risk of attack which is inherent, substantial and unavoidable.

64. First, there is the size and complexity of the network, in terms of geographic reach and the numbers of trains, stations and commuters involved. Would-be attackers have a great number and variety of potential targets.

65. Second, reducing journey times and increasing the speed with which customers enter and exit tube stations are vital to the effective operation of London Underground. Time is the core value used to guide planning activity, with journey time being one of the primary measures by which the performance of the system is assessed. This means that whereas security screening equipment of the kind used at airports might well be very effective for London Underground's security purposes, it is not feasible because of the delays it would cause to travel.

66. Third, London Underground is an 'open' transport system. Customers can use it without disclosing their identity (again, unlike the case of air travel). Would-be attackers are thus generally able to avoid being identified or 'tracked'. A great deal of information about London Underground is publicly accessible. In part, this comes from the ability to enter tube stations and to observe those parts of the tracks which are visible in stations or above ground. More importantly, London Underground actively makes a great deal of information available to customers to assist with their travel arrangements. Information about maintenance, track replacement and so on is made available for the convenience of customers. So too is information about journey times, schedules and timetables. Train arrival and departure data is made publicly available: 'Trackernet' data. It helps customers and also facilitates the development of 'apps' (i.e. applications for mobile phones and tablet computers) which tell users when the next train to their destination is due, and helps them plan their journey using 'live' data. Mr Clack says there is an obvious and strong public interest in publishing such information, not only for customers' convenience but also to allow the public to hold TfL to account. TfL, he says, is committed to being as transparent as is compatible with safeguarding the security of the network and its users.

67. London Underground, in common with many other rail networks, attracts intense interest among train and transport enthusiasts, many of whom compile very detailed and often very technical data on London Underground trains, stations, infrastructure and operations. There are many websites and books which share such information for the purposes of interest and hobbies.

68. All of the above contribute to the 'openness' of London Underground: anyone can use publicly accessible information to learn a great deal about its operations.

The importance and challenges of emergency planning

69. Mr Clack says that one major consequence of the openness of London Underground is that while it can reduce the likelihood of an attack, it has to acknowledge that not all attacks can be prevented. Contingency and emergency response arrangements aimed at minimising the consequences of an attack are therefore as important as preventive measures in its security strategy.

70. The key here is to have plans in place for moving people away from points of risk. If an attack happens or is thought to be imminent, then tried and tested evacuation plans are in place to enable people to be moved out of the system. These plans range from a relatively straightforward evacuation of a single station at one extreme, to the total evacuation of the whole network, as was needed in July 2005, at the other.

71. While moving customers away from danger, London Underground also have to plan simultaneously for the emergency services to reach the scene rapidly. Reviews following the attacks in July 2005 highlighted the need to ensure quick access with appropriate tools, and the London Ambulance Service has, for example, subsequently made changes to its operations in order to address any future incidents on the London Underground.

72. Evacuation and emergency services access presents particular challenges for London Underground: getting to trains is much more complex with underground trains in tunnels, and the train density is higher than would be the case for overground trains.

73. At any given time there may be a number of trains between each station. Each train can have over 850 people on board. As was the case in July 2005, there is a real risk of attacks being made simultaneously at a number of points on the network. There is also a real risk of attacks being made sequentially, with short intervals between incidents, making it difficult to predict when the period of imminent risk has passed.

74. Evacuation is likely to involve trains being moved in the wrong direction, via routes that are not normally used in day-to-day service. In the

aftermath of an attack, trains are likely to be moved to positions they would not normally occupy in the ordinary course of their daily journeys.

75. In Mr Clack's view the requested information in this case would be a necessary component for building a 'simulator' or model allowing for accurate predictions about train movements and positions in these highly unusual emergency situations. Those predictions cannot be made using only the information that is already publicly available: the publicly available information is about 'business as usual' train movements, rather than emergency response movements. That is why TfL is extremely concerned at the prospect of having to disclose the requested information. Its concern accords with its information security strategy.

TfL's approach to information security

76. A further consequence of the openness of London Underground as described by Mr Clack explains, is that, with so much detailed information being publicly accessible already, TfL has to be very careful about where it 'draws the line'. In other words, it discloses as much information as possible up to the point where disclosure creates a real incremental security risk. In doing so – recognising the public importance of maximising transparency where possible – TfL conducts a balancing exercise, weighing up the significance of the incremental risk, the seriousness of the consequences of that risk materialising, and the public benefit in disclosure. In some cases, the probability of an attack may be relatively low, but the consequences would be so serious that the balance favours non-disclosure. In other cases, the information would obviously assist a would-be attacker, but the public interest (for example, in the ability to manage one's journeys) outweighs that risk.

77. For some information, this balancing exercise is straightforward. TfL obviously withholds information which would of itself be useful to potential attackers, unless there is some good public interest reason for disclosure.

78. In other cases (as in the present one) the risk arises not so much from the particular information viewed in isolation, but from how it may be combined with other accessible information to build up a cumulative picture or 'mosaic' which could be used to draw inferences and conclusions useful for planning attacks. Advice received from the Government security regulator has emphasised this 'mosaic effect', which is increasingly important in informing TfL's disclosure decisions.

79. Freedom of Information requests provide one means by which parts of the information 'mosaic' may become publicly accessible for potentially harmful actions. Train enthusiast websites and publications are another. TfL employees also need to know a lot of non-public information and while its employees are increasingly alert to security risks (including the risk of disclosing sensitive information), this 'leakage' cannot be entirely eliminated.

80. TfL has an Information Security strategy to help it make proportionate and well-informed decisions and to eliminate unnecessary security risks, legal difficulties and so on. The strategy is evolving, and is more mature in some areas than in others. For example, the protection of personal data has received close attention for many years and is a well-established area of TfL information governance. To take an example of the opposite kind, TfL's large and complex portfolio of physical assets and infrastructure means it holds thousands of technical documents, plans, drawings and similar information. TfL's classification and management of those sorts of information is comparatively less mature.

81. In TfL's view, disclosure of some technical information in the past should not be seen as setting a precedent for disclosure of other technical information such as the requested information in this case. Mr Clack is not aware of any particular past disclosures that could be considered a precedent, but if there were any – and if it were sufficiently similar to the requested information in this case – he would simply say that TfL's decision-making on such issues evolves and improves. Some information disclosed in the past is likely to have become out of date, whereas information disclosed now would be up to date by reference to the time of the request. He is confident that at the time of this particular request TfL made the right decision, because the incremental risk created by the contribution of this information to the 'mosaic' available to the would-be attacker is substantial, and in his view outweighs any public interest in disclosure.

82. TfL's Information Security strategy addresses both 'internal' and 'external' disclosure. On the internal front, it includes a relatively recently developed classification system to ensure that information is understood in terms of its security relevance and then treated accordingly. TfL have evolved what can be best described as a three-tier approach. The most critical information is controlled so as to ensure that only those with a 'need to know' can access it. Other information is widely available internally because many employees need it to do their jobs. Between these extremes is a category of information which can be accessed only by specified employees whose role requires that information (such as information on TfL databases and other computer systems) or upon a well-founded request (such as information produced and held by internal technical specialists).

83. Mr Clack also makes clear that there could be instances in which TfL would be minded to refuse a request even where the information could, with sufficient effort on the part of a member of the public, be obtained anyway – for example by attending relevant sites in person and carefully recording observations. This is because, in such cases, TfL have been informed by its police advisors that the planning or reconnaissance stage provides an important opportunity for potential attackers to be noticed (for example, on CCTV or by staff) and apprehended. This preventive opportunity is lost with FOI requests, given the ease with which they can be made anonymously.

84. In those types of case, TfL's approach may be summarised in this way: it cannot fully prevent an attack, but it can make it harder, riskier or less attractive to plan. It would be irresponsible, in Mr Clack's view, to adopt an opposite approach which said in effect 'we cannot fully prevent an attack, so we might as well disclose further details'.

85. Finally Mr Clack informs us that if the disputed information is disclosed the risk of a terrorist attack is very real. It is far from remote, hypothetical or speculative. In fact, the stated motivation for this request is for the requested information to be used to build a simulator, which is intended to be sold commercially, as a hobby item for train enthusiasts who would value particularly accurate simulators. He is not suggesting that the requester has any malicious intent whatsoever. The reality is, however, that disclosure of the requested information would result in (or at least make a significant contribution towards) an accurate simulator which uses track speed limit data to allow for the modelling of emergency situations being made available for purchase or use by someone who did wish to do harm to the London Underground.

Terrorists' research and accumulation of information

86. Mr Dwyer informs us that the terrorist is likely to strike when he is sufficiently confident that his plan will be successfully implemented, and when he has identified sufficiently attractive targets. In many cases, the attractiveness of a target is measured by how much damage (including death and injury) can be caused (hence attacks being made at peak times), the public profile of the target and the openness of the target environment.

87. A terrorist's objectives will be measured in terms of loss of life, atmosphere of terror created, economic damage and publicity given to the terrorist's cause.

88. The terrorist's confidence in success is built up through careful planning. A major aspect of such planning is the diligent gathering of as much detailed information as possible about the target, for example the London bombings of 2005 where the attackers are well known to have undertaken research exercises[2].

89. Terrorists are not only interested in gathering as *much* data as possible to facilitate their planning. They are particularly interested in *high quality* data. The more accurate, the more useful for predictions and planning. The more technical the better. Officially-confirmed information is much more valuable than speculation or inference.

[2] For example, the *House of Commons Report of the Official Account of the Bombings in London on 7th July 2005* (HC 1087) page 24, paragraph 65.

90. Mr Dwyer says the present case is about the disclosure of technical, accurate and officially-confirmed data which, by means of the simulator described by Messrs Clack and Apostole, would be, in his view, of great assistance in planning attacks.

The mosaic effect and the need for vigilant analysis of disclosures

91. Through diligent research and on-site reconnaissance (referred to in police parlance as 'hostile reconnaissance') much can be learned about an open mass-transit system. Mr Dwyer accepts that, to some extent, very little can be done about that sort of information-gathering. That, however, does not justify providing the potential terrorist with useful and otherwise unavailable information.

92. He argues for the opposite: the wide availability of so much observable and otherwise obtainable information is a reason to be more rather than less cautious about disclosure of information such as that requested in this case. Requests for technical and non-observable information such as this should be given serious consideration and not simply acceded to because, at first glance, the information appears harmless in and of itself.

93. A further important point made by Mr Clack, which Mr Dwyer fully endorses: in cases such as the present, what matters is not the risk posed by this information alone. Rather, what matters is the 'mosaic effect', i.e. how this particular information could be combined with other open source information so as to build up a cumulative picture from which a terrorist could draw helpful inferences and conclusions to support his plans.

Diminished opportunities for interception

94. Mr Dwyer considers that simulators of the accuracy described by Mr Clack would not only make the terrorist's planning job much easier. It would also allow much of the information-gathering to be done safely and anonymously, without having to visit potential targets in person and make physical observations. This sort of on-site hostile reconnaissance activity is closely monitored by British Transport Police. It provides a very important opportunity to intercept and act upon potential attackers. Special Branch of British Transport Police, for example, has investigated several reports of suspicious activity involving people timing train movements with stop watches.

Targeting of emergency services

95. Mr Dwyer explained that an acknowledged tactic of terror groups the world over is to use one attack to drive those fleeing from its effects into an area of even greater danger: a tactic sometimes referred to as 'secondary

devices'.[3] In Mr Dwyer's view the production of the simulator at issue in this case would substantially increase an adversary's ability to predict the response and movements of the emergency services and to plan so as to undermine or exploit those responses.

The importance of confidence

96. Mr Dwyer emphasised the value in the overall mosaic of information to a terrorist, because of its high-quality and being officially-confirmed technical data. He acknowledges that Mr Clack's evidence explains the key point for this case, namely that this information would allow for the building of a simulator which accurately models responses in unusual, emergency conditions.

97. The ability of terrorists to predict train movements with a high-level of accuracy necessarily increases the overall likelihood of an attack, particularly given the inherent vulnerability of open systems such as mass-transit rail. By being able to predict where and when trains will be held and disembarked, and where displaced people are likely to gather in great numbers as a result, such information provides terrorists with a level of planning which is *not otherwise available*. The information in this case offers a level of precision which cannot otherwise be arrived at.

98. Mr Dwyer adds this important point: what matters is not so much whether the terrorist's predictions are *in fact* accurate. What matters is that he is sufficiently *confident* in their accuracy so as to decide that his plan is worth carrying out. A model which would rightly be able to claim a high degree of accuracy because of its detailed technical inputs about track speed limits would be just the sort of tool which is likely to bolster, to a very meaningful extent, the potential terrorist's confidence in the robustness of his plan to maximise damage. Confidence, coupled with detailed planning, is often the trigger to acting on such plans.

99. Mr Dwyer considers that accurate technical data of the type at issue in this case is an important component in formulating countermeasures to terrorism, particularly as regards chemical attacks.[4] To disclose this information undermines the advantages TfL seek to build over potential adversaries.

100. He contends in very strong terms that disclosure of the disputed information would represent a real and substantial additional risk of an attack on the London Underground, given how valuable such accurate technical data would be, once fed into a simulator, in bolstering potential terrorists' confidence in their plans.

---

[3] This was noted in a Ministry of Defence paper (*Military Perspective on the Civilian Response to the London Bombings July 2005;* SA Bland, DJ Lockey, GE Davies, AD Kehoe, *J R Army Med Corps 2006; 152: 13-16*) at page 14.

[4] See for example the BBC article *'Poison gas' test on underground* available at http://news.bbc.co.uk/1/hi/england/london/6492501.stm) .

101. Mr Dwyer drew an analogy with a point made by the Director General of the Security Service, who noted in the *Intelligence and Security Committee Report into the London Terrorist Attacks on 7 July 2005 (Cm 6785)* that when gathering intelligence (whether as a terrorist or a counter-terrorist) "…*some is gold, some dross and all of it requires validation, analysis and assessment"* (page.7, paragraph 19). In his view, the simulator (for which the disputed information is an important component) is, given the accuracy it offers about predicted train movements in the event of service disruption, equivalent to presenting aspiring terrorists with "gold".

102. He said to the Tribunal that it would "unquestionably" make his job more difficult if the disputed information was disclosed.

Whether the section 24(1) exemption is engaged?

103. The section 24(1) exemption from section 1(1)(b) FOIA is engaged if it is "required for the purpose of safeguarding national security".

104. Mr Capewell for the Commissioner strongly argues that the disputed information in itself is not material and that the likelihood of the risk of attack is small. He contends that TfL does not meet the causation test and that it is applying misplaced caution. He asked us to consider whether there is a real possibility that disclosure of the disputed information would adversely affect national security in this case. He argues that a remoteness test as to a real possibility of attack should be applied. He contends that there is insufficient evidence that there is a real possibility of attack and that the disclosure of the disputed information would not tip the balance. He says that it is important to look at what has actually happened in the past and that a simulator has not been used in the circumstances suggested in evidence in this case. He argues that the witnesses in this case are not experts as such and that we should consider the evidence objectively. Among other arguments he contends that TfL are trying to stop disclosure too early and there are still other important pieces of information missing such as positions of signals, dwell times etc. before the TfL simulator could be accurately replicated.

105. Mr Capewell also contends that the test under section 24(1) is that there must be a clear basis for arguing that disclosure would have an adverse effect on national security if the exemption is to be engaged. However this is a class based exemption. There is no harm, prejudice or adverse effect test as such as with some other qualified exemptions. The House of Lords in *Rehman* was dealing with a different statute and a very different set of facts. Section 24(1) is engaged if it is "required for the purpose of safeguarding national security". This is a different test which other Tribunals have considered in terms of whether the exemption is "reasonably necessary" for the purposes of safeguarding national security. We consider that this is the right approach.

106. We have considered the arguments and the detailed evidence set out above.

107. Clearly London Underground is the transport hub of the nation's capital. As such it has been and still is a major security risk from terrorist attack.

108. We have heard detailed evidence that the disputed information if made available would enable commercial publicly available simulators to be even more accurate in replicating the emergency planning process undertaken by TfL with its own in-house simulator. There will still be some missing ingredients, but we are informed by very knowledgeable witnesses that in their considered view it would go a step too far in providing information which could both help terrorists to plan and undertake an attack on the London Underground, in this case the Victoria Line, and also to give terrorists greater confidence to embark on such an exercise.

109. We find that particular weight should be afforded to these views as the witnesses have provided an extremely convincing assessment of what is required to safeguard national security in the circumstances of this case. Although we heard no evidence that an attack was certain or immediate, (and we would not expect to be provided with such evidence), we are convinced from the evidence that a terrorist attack is a credible and real possibility.

110. Although much travel type information is already in the public domain because of the nature of London Underground as a public transport system, there is a balancing point where further information does not necessarily contribute to improved use of the system by the population at large but does provide improved means for terrorists to undertake an attack on the Victoria Line of national security proportions.

111. From the evidence in this case the disputed information appears to us to be at a tipping point where there is a serious risk that if disclosed it would pose a real threat to our national security. In coming to this conclusion we have taken into account Baroness Hale's words of caution in *MB v Secretary of State for the Home Department* at paragraph 20 but have borne in mind the context of the facts in that case which are very different from the facts in this case.

112. Therefore we find, based on the evidence, that preventing more accurate simulators from entering the public domain is reasonably necessary for the safeguarding of national security. We find that the section 24(1) exemption is engaged and now turn to the public interest test.

Public interest balance

113. Section 24 is a qualified exemption so we need to consider the public interest test under section 2(2)(b) and whether "in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information".

114. The Commissioner says that if we find that the exemption is engaged then he does not challenge the TfL's position that the public interest balance favours maintaining the exemption, although Mr Capewell contends there are public interest factors in favour of disclosure. We can understand this position.

115. From the above evidence and our finding that the exemption is engaged we consider there is an inherently strong public interest in maintaining the exemption under section 24(1). Any real risk to national security must be a very weighty public interest factor. In this case the structure of the Victoria Line (being underground except for depots) and the number of travelling passengers in confined spaces makes it particularly vulnerable to terrorist attack. The fact that the disputed information in itself is anodyne and is not the only missing information from a perfected replica of TfL's simulator, does not in our view lessen the weight of the public interest in favour of maintaining the exemption. It is part of that mosaic of information which creates a real risk to national security.

116. There is clearly a strong public interest in London Underground providing sufficient information for the travelling public to be able to plan its journeys and make the best of its travelling experience and to hold TfL to public account if London Underground is not running as it should. However it appears from the evidence that there is already sufficient information in the public domain for the necessary transparency and accountability. In this case it does not seem to us that the disputed information is necessary for actual travelling purposes or to hold TfL to account and therefore the public interest in its disclosure is thereby weakened.

117. Although this jurisdiction is considered to be "motive blind" there are in our view exceptions particularly where it goes to the strength of a public interest and national security is involved. If the requestor was a known terrorist there is no doubt we should take this into account. There is no such suggestion in this case and we make none. However we know that the requestor has developed a simulator for train enthusiasts which he provides online on a commercial basis. There is a public interest in him being able to provide a simulator which provides these enthusiasts with a realistic modelling experience. Although we were not provided with any evidence on the matter we consider that it is commonsense that such enthusiasts will be small in number particularly compared to the number of people travelling on the Victoria Line. Therefore we cannot give much weight to this public interest factor particularly where the provision of the

disputed information, however anodyne in itself, has the potential to increase the risk of a terrorist attack.

118. Therefore we find that the balance of public interest favours maintaining the exemption.

Conclusion

119. As we have found that the section 24(1) exemption is engaged and the public interest in maintaining the exemption outweighs the public interest in disclosure we do not need to consider the section 38 exemption.

120. Therefore we allow the appeal and find that TfL is not required to disclose the disputed information.

121. Our decision is unanimous.

Dated: 28 February 2013

John Angel Judge