Report Published under Section 48(1) of the Personal Data (Privacy) Ordinance (Cap. 486)

Report Number: R13-2768

Date issued: 9 April 2013

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

This page is intentionally left blank to facilitate double-side printing

Report on the Inspection of the Personal Data System of the MTR's CCTV System

This report of an inspection carried out by the Privacy Commissioner for Personal Data ("**the Commissioner**") pursuant to section 36 of the Personal Data (Privacy) Ordinance, Cap. 486 ("**the Ordinance**") in relation to the Closed Circuit Television system used by the MTR Corporation Limited ("**MTR**") in train stations and compartments is published pursuant to section 48 of the Ordinance.

Section 36 of the Ordinance provides that:-

"*Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of-*

(a) any personal data system used by a data user; or

(b) any personal data system used by a data user belonging to a class of data users,

for the purposes of ascertaining information to assist the Commissioner in making recommendations-

(i) to-

(A) where paragraph (a) is applicable, the relevant data user;

(B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and

(ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be."

The term "**personal data system**" is defined in **section 2(1)** of the Ordinance to mean "*any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system.*"

The relevant parts in **Section 48** of the Ordinance provide that:-

"*(1) Subject to subsection (3), the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report-*

(a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(b) in such manner as he thinks fit.

……

(3) Subject to subsection (4), a report published under subsection (1)… shall be so framed as to prevent the identity of any individual being ascertained from it.

(4) Subsection (3) shall not apply to any individual who is-

(a) the Commissioner or a prescribed officer;

(b) the relevant data user."

Allan CHIANG
Privacy Commissioner for Personal Data
Hong Kong SAR

Table of Contents

Executive Summary

Introduction

1. With the rapid technology advance in digital video imaging and recording, the use of CCTV in public places or common areas of buildings for security reasons or for general monitoring against illegal acts has become increasingly widespread. As simple CCTV systems are capable of capturing extensive images of or information relating to individuals, indiscriminate and / or unjustified use of CCTV will likely impact on the personal data privacy of individuals.

2. Serving millions of passengers[1] every day, MTR is the largest public transport service provider in Hong Kong. In February 2012, MTR had 1,967 train compartments, 429 or 22% of which were installed with CCTV, potentially covering an average of over 1 million passengers every weekday.

3. No doubt MTR train service has become an indispensable part of people's daily lives in Hong Kong. As such, members of the public would reasonably expect that the installation and use of the CCTV system are justified under the law, and comprehensive measures are in place to protect passengers' personal data privacy. On this basis the Commissioner considers that it is in the public interest to carry out an inspection (the "**Inspection**") of the CCTV system used in the MTR stations and train compartments (the "**CCTV system**") pursuant to section 36 of Ordinance, with a view to :

- Evaluating the integrity of the CCTV system;
- Making recommendations to MTR relating to the promotion of compliance with the provisions of the Ordinance; and
- Providing practical reference to other data users who intend to use or are using CCTV systems in their operations.

[1] In February 2012, MTR railway alone carried an average of 4.9 million passengers in Hong Kong every weekday.

The Inspection

4. The Inspection examined the CCTV system used by MTR to monitor the public areas of the MTR stations and train compartments. The Inspection involved four major areas of work:-

(a) Review of relevant MTR manuals / guidelines;

(b) Written enquiries with MTR;

(c) Interviews with key staff members involved in the operation of the CCTV system; and

(d) Onsite inspection of premises and equipment used for the CCTV system, including on-site observation of demonstration performed by MTR staff members.

Findings

5. The Inspection commenced in June 2012 and ended in February 2013. The major findings of the Inspection are:-

(a) The installation and use of the CCTV system were justified for the discharge of MTR's statutory and contractual obligations, having regard to its functions and activities;

(b) All CCTV cameras inspected by the Commissioner's officers were overtly installed and visible;

(c) There was proper control over the provision of CCTV footages to third parties, such as law enforcement agencies;

(d) However, MTR has never conducted a systematic privacy risk assessment for the CCTV system;

(e) CCTV notices were insufficient and inadequate in terms of both quantity and quality;

(f) The information about the CCTV system as set out in "*Travel Safely Everyday in the MTR*" booklet was too brief;

(g) No policy or procedures had been promulgated to guide staff concerned on how CCTV footages or copies thereof should be erased; there was no regular exercise or formal record of erasure of CCTV records kept by MTR's Operations Safety Section; erasure where performed was conducted randomly at the discretion of individual staff members;

(h) Certain CCTV images were kept longer than the retention period prescribed by MTR;

(i) The login account and password of the Digital Video Recording System was shared among staff members of the Operations Safety Section. This arrangement is not conducive to user accountability and data security;

(j) A USB thumb drive without encryption was used for copying, storage and transfer of personal data captured by the CCTV system; and

(k) Personal data privacy policies and procedures were scattered in many different kinds of internal manuals.

Recommendations

6. The following recommendations are made in light of the Inspection findings:-

(a) A privacy impact assessment ("**PIA**") should be conducted to help identify and address potential privacy issues;

(b) Consideration should be given to the visibility and sufficiency of the CCTV notices and the information therein to ensure they are

prominently and conspicuously displayed with all the necessary details;

(c) The "*Travel Safely Everyday in the MTR*" booklet should be reviewed and refined to provide more information on the CCTV system;

(d) The Personal Information Collection Statement ("**PICS**") contained in the "*Travel Safely Everyday in the MTR*" booklet and on the MTR website, and MTR notices at entrances and exits to station premises, should be reviewed and refined so that MTR passengers can be better informed of the PICS;

(e) Policy and procedures on the erasure of CCTV records or copy CCTV records should be formulated and carried out by fully trained staff who are conversant with the procedures;

(f) Access to computer recording and storage of CCTV footages should not be shared to ensure accountability and data security;

(g) Policy and procedures on the use of portable storage devices (e.g. USB thumb drive) should be enforced to prevent possible unauthorized access or loss of CCTV footage in transit; and

(h) Consideration should be given to streamline and consolidate all data privacy policies and procedures, instructions and guidelines, and to review or align the disparity between retention periods of CCTV records among different railway lines. This will promote compliance and user-friendliness and to facilitate training..

Chapter One

Introduction

The Issue

1.1 The use of CCTV[2] in public places or common areas of buildings for security reasons or for monitoring illegal acts[3] has becoming increasingly widespread. However, since CCTV may capture extensive images of individuals or information relating to individuals, indiscriminate use of CCTV inevitably risks intrusion into the privacy of individuals.

1.2 In the public transport arena alone, over 11 million passenger journeys are made every day in Hong Kong. Of these, out of a total of 347 MTR trains 78 have been installed with CCTV[4]; out of a total of 5,800 franchised buses 1,580 have been installed with CCTV and all 163 trams in service have been installed with CCTV in their tram compartments[5].

1.3 As a result of experiences consolidated from consultation by many organizations and government departments on the use of CCTV surveillance practices in public areas in the past years, the Office of the Privacy Commissioner for Personal Data (the "**PCPD**") published a Guidance Note on CCTV Surveillance Practices (the "**Guidance Note**") in July 2010 with a view to offering advice to organizations on whether CCTV should be used, how to use it responsibly and helping them understand the requirements under the Ordinance relating to the collection and proper handling of personal data.

1.4 The Guidance Note also provides practical guidance to organizations

[2] "Closed Circuit Television" – camera surveillance systems or other similar surveillance devices

[3] Covert surveillance conducted by a law enforcement agency is regulated by the Interception of Communications and Surveillance Ordinance, Cap. 589.

[4] Although MTR has no plan to install CCTV in train compartments that have not yet been installed with CCTV, all new trains will be installed with CCTV as standard technical specification, as in the case of other international train operators, according to the information provided by the Secretary for Transport and Housing, Ms. Eva Cheng at the Legislative Council Meeting on 11 January 2012.

[5] Information and figures were extracted from the written reply by the Secretary for Transport and Housing, Ms. Eva Cheng to Legislative Council to question no. 12 on Installation of CCTV cameras in public transport vehicles raised by the Hon Wong Sing-chi at the Legislative Council Meeting on 11 January 2012.

including :-

1.4.1 The positioning of CCTV camera and notices;
1.4.2 The proper handling of recorded images;
1.4.3 The transfer of CCTV records to third parties; and
1.4.4 The transparency of CCTV monitoring policy and practices.

1.5 From a regulatory perspective, PCPD considers that a proper balance should be struck between the protection of public interests and personal data privacy when using CCTV in public places. Data users should handle the issues in a fair and transparent manner giving due regard to personal data privacy.

Background of MTR

1.6 MTR is a publicly listed company in Hong Kong Stock Exchange. It is independently managed under commercial principles and is financially independent of the Hong Kong Special Administrative Region Government (the "**Government**"). Around 77% of MTR shareholding is held by the Government[6].

1.7 MTR operates rail based transportation system in Hong Kong, comprising domestic and cross-boundary services, airport express railway and a light rail system. It operates the following rail lines :-

1.7.1 Kwun Tong Line running between Yau Ma Tei and Tiu Keng Leng;
1.7.2 Tsuen Wan Line running between Tsuen Wan and Central;
1.7.3 Island Line running between Sheung Wan and Chai Wan;
1.7.4 Tseung Kwan O line running between Po Lam / LOHAS Park and North Point;
1.7.5 Tung Chung Line running between Tung Chung and Hong Kong;
1.7.6 Airport Express running between Asia World Expo and Hong Kong;
1.7.7 Disneyland Resort Line running between Sunny Bay and

[6] http://www.mtr.com.hk/eng/overview/profile_index.html dated 21 January 2013.

Disneyland Resort; and

1.7.8 East Rail Line running between Hung Hom and Lo Wu / Lok Ma Chau;

1.7.9 West Rail Line running between Hung Hom and Tuen Mun;

1.7.10 Ma On Shan Line running between Tai Wai and Wu Kai Sha; and

1.7.11 Light Rail Lines running communal services in the north-west territory.

1.8 In February 2012, with its 1,967 train compartments MTR railway carried an average of 4.9 million passengers[7] in Hong Kong every weekday. Of these, 22% or 429 train compartments were installed with CCTV, covering on average of over 1 million passengers every weekday.

Rationale for Inspection

1.9 Supporters for the use of CCTV argued that surveillance in trains is highly desirable for maintaining better safety and security control because MTR trains have become increasingly crowded nowadays thus adding to the risk of crimes, such as pick pocketing, sexual assaults and other crimes in train compartments[8]. Whilst having more uniformed police patrols in stations and on trains might be useful, the limited number of police officers and the very crowded conditions in train compartments often constrain effective deterrence of crimes and sexual assaults. The installation and use of CCTV might deter crime, detect accidents, facilitate prompt action in case of notifiable occurrences, incidents and / or emergencies occurring in stations and train compartments.

1. 10 Detractors of the use of CCTV on the other hand, argued that surveillance in trains is an intrusion of privacy. Other arguments include that: less privacy intrusive alternatives have not been considered or seen to be considered; there is no evidence that shows that the effectiveness of use of CCTV in stations and train compartments have been reviewed, scrutinized and monitored to prevent abuse or misuse, etc.

---

[7] http://www.mtr.com.hk/eng/overview/profile_index.html dated 21 January 2013.

[8] See e.g. Hong Kong Headline dated 6 March 2013; Singtao Daily dated 8 February 2013; Sina Online News dated 13 September 2012.

1.11 Having considered the fact that :-

1.11.1 MTR is the largest public transport service provider in Hong Kong;

1.11.2 the great number of data subjects affected; and

1.11.3 the freedom of MTR passengers in choosing not to supply their personal data to MTR

the Commissioner considered it appropriate for him to carry out an inspection of the installation and use of CCTV on station premises with public accessibility and in train compartments pursuant to section 36 of the Ordinance for the purposes of :-

1.11.4 Evaluating the integrity of the CCTV system;

1.11.5 Making recommendations to MTR relating to the promotion of compliance with the provisions of the Ordinance; and

1.11.6 Providing practical reference to other data users who intend to use or are using CCTV systems in their operations.

Chapter Two

The Inspection

Commencement of the Inspection

2.1 In response to media reports on MTR's intention to install CCTV in train compartments for security purposes and provision of assistance to passengers, PCPD wrote to MTR on 15 January 2008, urging it to strictly comply with the requirements under the Ordinance to safeguard the personal data privacy of the public when using CCTVs in train compartments[9].

2.2 With the increasingly common and widespread usage of CCTV monitoring and recording system in public places, in addition to advocating compliance with the Ordinance, the Commissioner felt the need to guide data users on the use of CCTV. On 22 July 2010, PCPD published a Guidance Note with a view to offering advice to organizations on whether CCTV should be used, how to use it responsibly, and to help them understand the relevant requirements under the Ordinance relating to the proper handling of the personal data.

2.3 Two years have elapsed since the publication of the Guidance Note CCTV has become a standard equipment for all new train compartments procured, supplied and put into service by the MTR. To assess the integrity of the MTR personal data system, on 26 June 2012 in accordance with section 41 of the Ordinance, the Commissioner informed the MTR in writing of his intention to carry out an inspection of the personal data system of their CCTV monitoring and recording system.

[9] PCPD media statement dated 15 January 2008.

The Inspection Team

2.4 An inspection team (the "**Team**") consisting of five officers[10] from the Compliance & Policy Division of the PCPD was formed to carry out the Inspection.

Pre-Inspection Meetings

2.5 The Team held two meetings with MTR staff on 31 May and 14 September 2012 to introduce, explain and clarify the nature, purposes, scope and methodology of the Inspection, answer MTR's queries and addressing it's concerns, and gain understanding of the logistics and operations of the MTR personal data system with respect to the installation and use of CCTV on station premises and in train compartments. The Team was given an overview of the MTR personal data system with respect to the use of CCTV covering :-

2.5.1 the purposes of the system;
2.5.2 operation of the system;
2.5.3 locations of the system;
2.5.4 types of CCTVs used;
2.5.5 notification of CCTV monitoring or recording;
2.5.6 recording function of CCTV;
2.5.7 retention of CCTV records;
2.5.8 use and transfer of CCTV records;
2.5.9 security of records;
2.5.10 access to records; and
2.5.11 erasure of records.

[10] The Team consisted of one Chief Personal Data Officer, one Senior Personal Data Officer, one Personal Data Officer and two Assistant Personal Data Officers.

Scope of the Inspection

2.6 The Inspection examined the integrity of the MTR personal data system by reviewing the use of CCTV on station premises with public accessibility and in train compartments. It also examined the applicability of the Guidance Note and compliance where appropriate by the MTR personal data system.

2.7 The scope of the Inspection was restricted to an assessment of the areas with public accessibility only. Owing to resource constraints, the Inspection covered only nine interchange or busy train stations of all the eleven rail lines, as well as two train depots where two trains with compartments installed with CCTV were parked. The findings of the Team were based on the documentation obtained, MTR's presentation, representations and the Team's observations at the time of the site inspections.

Methodology

2.8 The Team completed the Inspection under section 36 of the Ordinance by reference to information gathered from the following:-

Presentation

2.9 An interactive presentation by MTR staff on the MTR personal data system with respect to the installation and use of CCTV facilitated understanding of the system.

Enquiry

2.10 Before, throughout and after the site inspection, the Team made a series of written and verbal enquiries with the MTR with a view to understanding more fully the operations of the MTR personal data system with respect to the use of CCTV. The Team also made enquiries with MTR to ascertain information that may not have been spelt out or apparent from documents or records. Information thereby obtained assisted the Team in

understanding the operations of the personal data system with respect to the use of CCTV, in reconciling the documentary evidence obtained in the Inspection and in identifying any cause for concern. MTR was also able to make reciprocal enquiries to clarify or supplement the evidence in question to avoid misunderstanding or misinterpretation.

Manuals / Guidelines Review

2.11 Before, during and after the site inspections, the Team had closely examined and was guided by the MTR Administration Manual, Personal Data Privacy Compliance Manual, various information leaflets and other material to which various MTR departments had drawn references in the handling of their personal data system with respect to the use of CCTV. These documents laid down the foundation, direction and guidelines on procedures such as the viewing and retention of the CCTV records. Persons responsible for the personal data system with respect to the use of CCTV, including the Operations Safety Manager ("**OSaM**"), Group Station Managers and Station Controllers, were also required to observe the requirements stipulated in the manuals. Given the importance of the Administration Manual, the Team had scrutinized it and made extensive references to it throughout the Inspection.

Site Inspections

2.12 Visits to the station premises and train compartments in which personal data is collected and the premises where the collected data is processed, stored, retrieved and transmitted were the key part of the Inspection. The Team was also able to personally inspect the equipment used for collecting, processing and storing the personal data, and identify any issues that might not have been apparent from documents, other presentation or representations.

2.13 Between 26 November and 14 December 2012, the Team inspected :-

2.13.1 Nine interchange or busy train stations with high traffic volume but covering all of the eleven rail lines;

2.13.2 the Kowloon Bay and Siu Ho Wan depots, where train compartments of the Kwun Tong Line and of the Disneyland Resort Line with installation and use of CCTV were parked for inspection;

2.13.3 the MTR Headquarters ("**HQ**"); and

2.13.4 the MTR Tuen Mun Building, in which the personal data system with respect to the use of CCTV of the Light Rail was processed.

2.14 The dates of site inspections and sites inspected are set out below :-

Date	**Rail lines**	**Stations / Premises**
26 November 2012	Island Line	Wan Chai Station
27 November 2012	Island Line Tsuen Wan Line	Central Station
28 November 2012	East Rail Line Ma On Shan Line	Tai Wai Station
29 November 2012	West Rail Line Tsuen Wan Line	Mei Foo Station
30 November 2012		Kowloon Bay Depot
3 December 2012	Island Line Tseung Kwan O Line	North Point Station
4 December 2012	West Rail Line Light Rail Line	Tuen Mun Station MTR Tuen Mun Building
5 December 2012	Airport Express Line Tung Chung Line	Hong Kong Station
6 December 2012	East Rail Line Kwun Tong Line	Kowloon Tong Station
12 December 2012	Disneyland Resort Line Tung Chung Line	Sunny Bay Station Siu Ho Wan Depot
14 December 2012		Kowloon Bay HQ

Interviews

2.15 By interviewing the persons responsible for the implementation and security of the personal data system with respect to using CCTV, operational and logistical questions including the following could be discussed and clarified:-

2.15.1 the operation of the personal data system with respect to using CCTV;

2.15.2 the respective roles of the MTR staff responsible for the use of the CCTV system;

2.15.3 the practices in handling personal data and whether these were in compliance with the requirements under the Ordinance; and

2.15.4 whether the relevant policies and procedures of MTR were adequate.

2.16 Between 26 November and 14 December 2012, the Team interviewed the following staff of MTR :-

Date	Stations / Premises	Job Title of Interviewees
26 November 2012	Wan Chai Station	✧ Senior Station Control Officers
27 November 2012	Central Station	✧ Group Station Manager ✧ Shift Station Master
28 November 2012	Tai Wai Station	✧ Shift Station Master
29 November 2012	Mei Foo Station	✧ Shift Station Master
30 November 2012	Kowloon Bay Depot	✧ Train Crew Officer ✧ Two MTR Engineers
3 December 2012	North Point Station	✧ Shift Station Master
4 December 2012	Tuen Mun Station & MTR Tuen Mun Building	✧ Shift Station Master ✧ Manager, Passenger & Traffic Operations ✧ Traffic Officer
5 December 2012	Hong Kong Station	✧ Shift Station Master
6 December 2012	Kowloon Tong Station	✧ Shift Station Master ✧ Designated Senior Station Master
12 December 2012	Siu Ho Wan Depot	✧ Two Depot Staff
	Sunny Bay Station	✧ System Controller ✧ Senior Station Control Officer

Date	Stations / Premises	Job Title of Interviewees
14 December 2012	Kowloon Bay HQ	✧ Senior Operations Safety Officer ✧ Senior Legal Advisor ✧ Design Support Engineer from Technical & Engineering Services Department

Demonstration

2.17 In the course of interviewing the persons responsible for the implementation of the personal data system with respect to the use of CCTV, they were asked to demonstrate on site : -

2.17.1 the operation of the CCTV system, for example, the functions of the CCTV cameras;

2.17.2 how personal data collected by the CCTV was processed including but not limited to retrieval, copying and transferring of records containing personal data; and

2.17.3 the facilities used to process the personal data.

Chapter Three

Personal Data System and Data Flow of the CCTV System

An Overview of the Personal Data System

Statutory and Contractual Obligations

3.1 Under sections 33 and 34 of the MTR Ordinance, there are statutory regulations[11] and by-laws[12] that provide for :-

3.1.1 the investigation of accidents on the railway or on the railway premises, or in which the railway is involved; and

3.1.2 the safety of persons on the railway or on the railway premises.

3.2 Under section 11 of the MTR Ordinance, MTR is also obliged to maintain various records, including, for example, details of any incident causing a service breakdown of 20 minutes or more.

3.3 In addition, MTR has the statutory obligation under the MTR Regulations to notify the Secretary for Transport and Housing not only of any accident that occurs on a part of the railway[13], but also occurrences in which, for instance, a person:-

3.3.1 falls off a platform or crosses a railway line whether or not he is struck by a train;

3.3.2 falls out of a carriage during the running of a train;

3.3.3 falls between a train and a platform;

3.3.4 comes into contact with live overhead electric traction wires or other live electrical equipment;

3.3.5 suffers injury, which is reported to MTR, by the opening or closing of carriage doors at a station or by the operation of

[11] MTR Regulations (Cap. 556 sub leg. A).
[12] MTR By-laws (Cap. 556 sub leg. B) and MTR (North-west Railway) Bylaw (Cap. 556 sub leg. H).
[13] MTR Regulations, Regulation 2.

an escalator, lift or moving path used by the public as part of the railway; and

3.3.6 suffers injury, which is reported to MTR, as the result of any action of an employee or of a contractor with MTR[14].

3.4 Owing to these statutory and contractual obligations with the Government, MTR is bound to collect, record, store, retrieve, use, transfer, secure and erase a lot of personal data and has to operate, manage and control personal data systems, one of which was the installation and use of CCTV on MTR station premises and in train compartments.

CCTV System Construction

3.5 MTR installed and used 3,342 CCTVs at public areas of station premises and 429 CCTVs in train compartments.

3.6 MTR installed analogue and digital CCTV systems at public areas of station premises and digital CCTV system in train compartments. The analogue system is to be replaced by digital system by end of the first quarter of 2013.

3.7 Not all train compartments are installed with CCTV. Not all CCTV cameras installed are equipped with recording function or with their recording function activated[15].

Data Flow of the Personal Data System

Stage 1: Collection

3.8 MTR installed and used CCTVs at the public areas of station premises and train compartments as follows:-

[14] MTR Regulations, Schedule.

[15] During the course of Inspection, MTR has provided (a) the total number of CCTV cameras installed; (b) the number of CCTV cameras with recording function and (c) the number of CCTV cameras with recording function activated. In order not to defeat MTR's installation purpose, i.e. to maintain security of their services, the exact numbers of (b) and (c) are not disclosed in this report.

Where	How	Camera Location
(a)	Public Areas	
Heavy Rails	Images are captured by cameras round the clock.	Public area of all stations, including :- (a) Lifts (b) Escalators (c) Staircases (d) Entrances / exits, including emergency and night access entrances (Photos 1 and 2) (e) Platforms (Photo 3) (f) Gate areas (Photo 4) (g) Cash-In-Transit route
Light Rails		(a) Platforms of 22 stops[16] (b) Three junctions[17] along the rail lines
(b)	Train Compartments	
Disneyland Resort Line	Images are captured by the cameras when the train compartments are in service.	Inside train compartments
C-Stock Trains[18]		

Photo 1

Photo 2

Cameras installed at entrances.

[16] The 22 stops are: Tuen Mun Ferry Pier, Tuen Mun Hospital, Siu Hong, Leung King, Ming Kum, Tai Hing (South), On Ting, Tuen Mun, Pui To, Prime View, Hung Shui Kiu, Hung Tin Road Emergency Platform, Hang Mei Tsuen, Tin Shui Wai, Tin Shui, Chung Fu, Tin Wing, Tin Heng, Tin Yat, Hong Lok Road, Tai Tong Road and Yuen Long.

[17] The three junctions are: (1) Junction at Ming Kum Road, Tin King Road and Tsing Tin Road; (2) Unsignalised junction at Hung Shui Kiu, Hang Mei Tsuen and Tong Fong Tsuen; and (3) Unsignalised junction at Ngan Wai, Affluence and Choy Yee Bridge.

[18] C-Stock Trains means the trains that were made in Changchun, China.

Photo 3

Photo 4

Cameras installed at concourse and platform.

3.9 According to MTR, CCTVs were installed and positioned in a way so as not to intentionally intrude upon the privacy of MTR users as MTR has no practice or intention of compiling information of any MTR user.

3.10 Cameras have been installed at train compartments of C-Stock trains and of the Disneyland Resort Line. There is no train captain on board the trains on the Disneyland Resort Line. The System Controller, who is the remote driver also controls the operation of the CCTV system in the train compartment. The image records captured by the cameras on the Disneyland Resort Line are transmitted by wifi to a storing device located in the Sunny Bay Station. Although C-Stock trains are equipped with CCTVs with recording function, the function has not been activated and no image has been recorded so far.

3.11 MTR has posted CCTV recording and in operation[19] notices (Photos 5 and 6) in prominent and conspicuous places at the entrance level of each

[19] "CCTV OPERATION – Closed Circuit Television ("CCTV") surveillance cameras are in operation on these premises. The CCTV cameras on these premises are being used for security and surveillance purposes."

station premises in both English and Chinese to inform all persons accessing the station premises that CCTV surveillance is in operation. MTR has also posted a notice[20] next to each in-train compartment CCTV surveillance camera in both English and Chinese to inform all MTR users that CCTV surveillance is in operation (Photo 7). MTR also displays the notices on the notice boards of all Light Rail station platforms (Photos 8 and 9).

Photo 5

Photo 6

Notices of CCTV recording and in operation posted at entrances.

Photo 7

Notice in train compartments.

[20] Ditto.

Photo 8

Photo 9

Notices on the notice board of Light Rail station platforms.

3.12 MTR also advises users in its "*Travel Safely Everyday in the MTR*" booklet[21] that all public areas of the MTR are regularly patrolled by MTR staff and the police. Mirrors and CCTVs are located at strategic positions to assist in deterring crime.

Stage 2: Recording and Storage

CCTV on station premises

3.13 MTR stated that digital video image captured by CCTV is encrypted and recorded in the hard disk of a DVR and analogue video image captured by CCTV is recorded on VCR tape[22].

3.14 Recorded images in the DVR hard disk will automatically be overwritten by new recorded images upon expiry of the retention cycle (see paragraph 3.17 below). VCR tapes are serially numbered corresponding to the periods of retention (see paragraph 3.17 below) and recorded images on the VCR tape will automatically be overwritten on the re-cycled and serially-numbered VCR tape by the newly recorded images.

---

[21] http://www.mtr.com.hk/eng/publications/images/safetybooklet.pdf.

[22] All images captured by CCTVs on the Island Line, Kwun Tong Line, Tsuen Wan Line, Tseung Kwan O Line, Airport Express Line, Tung Chung Line, Disneyland Resort Line and the Light Rail are digital images recorded by DVR system and all images captured by CCTVs on the East Rail Line, West Rail Line and Ma On Shan Line, are either digital or analogue images recorded by DVR or VCR system.

CCTV in train compartments

3.15 Each C-Stock train is equipped with an in-saloon CCTV system enabling the Train Captain to monitor the real-time condition of the train compartments (Photos 10 and 11). Footages can be saved in hard disks which are kept in locked cabinets of trains for a few days before they are recorded over. Each Disneyland Resort Line train is equipped with a Video Server enabling transmission of live videos captured in train compartments for real-time monitoring by the System Controller; and footages are stored in a hard disk located at the Sunny Bay Station.

Photo 10

Photo 11

Real time monitoring by Train Captain of C-Stock Train.

Photo 12 Photo 13


CCTV cameras and notice in a train compartment of Disneyland Resort Line.

3.16 According to MTR, the computer system that stores these CCTV video footages is password protected and can only be accessed by authorized staff members. The room where such computer system is placed is locked and the cabinets storing the CCTV footages are always secured. Access to the CCTV footage is restricted to authorized persons only. Video images can be recorded in a CD or DVD, which are stored in a cabinet inside a locked room accessible only by authorized individuals. Separate copies of the CCTV footages are also kept by the MTR Operations Safety Section for record.

Retention Periods

3.17 According to MTR's Administration Manual, the retention periods of CCTV footages stored in different systems and locations are as follows:-

System / Line	Retention Period
The DVR system of all lines except East Rail Line, West Rail Line, Ma On Shan Line and the Light Rail	28 Days
The DVR and VCR System of East Rail Line and Light Rail	28 Days
The DVR and VCR System of West Rail Line and Ma On Shan Line	13 Days
In-train footages of C-Stock Train / Kwun Tong Line	5 Days
In-train footages / Disneyland Resort Line	10 Days
"Viewed" footages kept by Operations Safety Section	3 Years

Stage 3: Retrieval, Use and Transfer

3.18 MTR uses CCTV to help maintain the safety and security of train

stations. CCTV not only enables MTR staff to view real time situations in accident-prone areas, on railway premises, moving pathway, escalators and railway platforms, it also allows MTR to :-

3.18.1 prevent, deter and detect crimes;
3.18.2 manage crowds and traffic;
3.18.3 detect any accidents, notifiable occurrences, incidents and / or emergencies which occur on the railway premises; and
3.18.4 take prompt emergency actions in case of any accidents or crime.

3.19 To this end, MTR only permits the retrieval of CCTV images in limited circumstances, such as :-

3.19.1 incident investigation;
3.19.2 for safety reasons or security audit by an MTR senior official or Railways Branch – Electrical and Mechanical Services Department ("**EMSD**");
3.19.3 crime investigation and crime prevention by the Hong Kong Police and other law enforcement agencies;
3.19.4 investigation of a fire by the Fire Services Department;
3.19.5 investigation of a notifiable accident directed by the Secretary for Transport and Housing[23]; or
3.19.6 prosecution or legal proceedings by the Court Liaison Office, or external law firms, in limited circumstances.

3.20 MTR stated that retrieving CCTV images, including personal data, if any, is restricted to the minimum necessary. Data collection, use and transfer are therefore applied on a limited duration and very restricted basis.

Handling of viewing and copying requests

3.21 In general, all requests for viewing have to be vetted and approved by the OSaM before viewing can be arranged. For urgent requests or requests raised outside office hours, Duty Service Managers ("**DSM**") of respective lines are designated to vet and approve such requests. Upon approval by

[23] MTR Regulations, Regulations 2, 5 and 6 and Part 1 of Schedule.

senior authority, viewing and copying of the CCTV footages shall be arranged by designated personnel[24].

Type / Source of Request	Legal Screening	Vetting and Approval Authority for normal request	Vetting and Approval Authority for urgent or emergency request
MTR Internal Request		OSaM	DSM
Request by Police, EMSD, other law enforcement agencies			
Request by Court Liaison Office or external law firm for legal proceedings or prosecution	MTR Legal Department		
Other external request			

Source of Video Images	Viewing Location	Designated Authority for Viewing Arrangement
Island Line Kwun Tong Line Tsuen Wan Line Tseung Kwan O Line Airport Express Line Tung Chung Line Disneyland Resort Line	1. Operations Safety Section's AV Room at 15/F of the MTR HQ 2. Group Station Manager (GSM) Office 3. Train Crew Manager (TCM) Office 4. Operations Safety Manager (OSaM) office 15/F, MTR HQ 5. Police RAILDIST Office at Kowloon East Operational Base (KEOB)	OSaM DSM Station Controllers
East Rail Line, West Rail Line and Ma On Shan Line	1. Operations Safety Section's AV Room at 15/F of the MTR HQ 2. Group Station Manager (GSM) Office 3. Train Crew Manager (TCM) Office 4. Heavy Rail Stations	
Light Rail	MTR Tuen Mun Building	Manager, Passenger and Traffic Operations
C-Stock train in saloon	Kowloon Bay Depot	Operations Safety Section via Kowloon Bay Depot
Disneyland Resort Line in saloon	Sunny Bay Station	Operations Safety Section via Sunny Bay Station

3.22 In any event, no CCTV footage can be duplicated or passed to any party without good reason and justification agreed by the OSaM, the MTR legal department or, in case of an urgent request, by the DSM. If any reproduction of the CCTV images or footages is required, a proper record of the leasing of the video copies and reproduction will be kept by the OSaM. The Operations Safety Section shall maintain proper records of any duplication and leasing of video copies[25].

[24] MTR's Administration Manual Issue/Rev 1.9 September 2012, page 1A4-13, 14 and 15.
[25] MTR's Administration Manual Issue/Rev 1.9 September 2012, page 1A4-a15.

Source of Video Images	Duplication Arrangement
Island Line	Operations Safety Section should arrange to make a copy for the requester and keep the original copy under MTR custody
Kwun Tong Line	
Tsuen Wan Line	
Tseung Kwan O Line	
Airport Express Line	
Tung Chung Line	
Disneyland Resort Line	
East Rail Line, West Rail Line and Ma On Shan Line	Carried out at stations via the Station Controller concerned
Light Rail	MTR Tuen Mun Building
C-Stock train in saloon	Arranged separately by Operations Safety Section via Kowloon Bay Depot
Disneyland Resort Line in saloon	Arranged separately by Operations Safety Section via Sunny Bay Station

Stage 4: Erasure

3.23 In addition to overwriting automatically the recorded digital CCTV images in the DVR hard disk by new recorded images upon expiry of the retention cycle, VCR tapes are serially numbered corresponding to the days of retention and recorded images on the VCR tape will automatically be overwritten on the re-cycled and serially-numbered VCR tape by the newly recorded images.

3.24 Upon expiry of the retention periods stated above in paragraph 3.17, all CCTV records would be destroyed following the requirements under the MTR Corporation General Instruction CGI241 - "Protection of Classified Corporation Information"[26].

Form of Storage	Means of Erasure
VCR tapes, CD, DVD	Recorded images in the VCR tapes will automatically be overwritten by new recorded images. Physically destroyed to prevent recovery, e.g. shredded before disposal. Large quantity should be packed for collection and disposal by designated contractor.
DVR files stored in hard disks, flash memory cards and USB thumb drives, etc.	Recorded images in the DVR hard disk will automatically be overwritten by new recorded images; or destroyed in a way rendering them unreadable. Destruction of storage media or hard disk must be sent to MTR IT Department for degaussing. If for any reason, the above is not feasible, the device / storage media must be physically destroyed to prevent the recovery of the classified information.

[26] MTR Corporation General Instruction on the Protection of Classified Corporation Information CGI241 dated 13 January 2010; MTR's Administration Manual Issue/Rev 1.9 September 2012, page 1A4-a15.

Chapter Four

Findings and Recommendations

Preliminaries

4.1 The findings and recommendations made in this report are based on the information provided by the MTR, and the observations, evaluation and review of the Team.

4.2 The following questions were posed in the Guidance Note to assist the data user in understanding the relevant provisions of the Ordinance and provide practical guidance concerning the use of CCTV. They are used in this section to evaluate the personal data flow of the MTR CCTV system :-

4.2.1 Is the use of CCTV necessary?
4.2.2 Has any privacy impact assessment been conducted ?
4.2.3 Where are the CCTVs and notices positioned ?
4.2.4 Are the recorded images handled properly ?
4.2.5 How are CCTV records transferred to third parties ?

4.3 In addition to the personal data flow, the privacy policy and practice of MTR in respect of CCTVs would also be assessed in this section.

4.4 The Team noted that MTR, in response to the enquiries of this Office, reiterated that they have no practice or intention of compiling information about any MTR user[27]. The Team, however, is of the view that the requirements under the Ordinance apply to MTR in the course of handling CCTV data, as the compilation of information about an individual is inevitable in some circumstances. For example, MTR may use CCTV records for incident investigation or when handling civil claim cases relating to MTR users. In these cases MTR would be compiling information about the relevant users

[27] According to the ruling of the Court of Appeal in *Eastweek Publisher Limited and Another v. Privacy Commissioner for Personal Data* [2000] 2 HKLRD 83, it is of the essence of the required act of personal data collection that the data user must thereby be compiling information about an identified person or about a person whom the data user intends or seeks to identify. If there is no collection of personal data, the data protection principles in the Ordinance would not be engaged at all.

whom MTR has identified or intends to identify. MTR CCTV records may also relate to a vast number of individuals who may be targets of investigation of law enforcement agencies or other organizations.

Findings

Personal Data Flow

Stage 1: Collection

Is it necessary to use CCTV ?

4.5 **Data Protection Principle ("DPP")1(1)** of the Ordinance requires that personal data shall only be collected where it is necessary for a lawful purpose directly related to the function or activity of the data user and that the data collected shall be adequate but not excessive.

4.6 In assessing whether it is necessary to use CCTV, the primary question is :- "*Is the use of CCTV in the circumstances of the case justified for the performance of the lawful function and activity of the organization and whether there are less privacy intrusive alternatives*[28]?"

4.7 MTR has both the statutory and contractual obligations to operate and maintain a safe, secure and efficient mass transit railway services but that does not per se give them the right to install and use CCTVs.

4.8 CCTV provides the functions of monitoring and recording of the coverage where the CCTV is positioned. In the performance of its statutory and contractual obligations, MTR is required to monitor pre-incidents and investigate post incidents. MTR may deploy staff to monitor all areas round the clock but staff may not be able to access crowded train compartments or other difficult to reach locations. MTR may also obtain evidence from witnesses of an incident and collect circumstantial or other supplementary information to facilitate its post incident investigation. MTR may still be able to perform its statutory and contractual obligations but it may not perform that well without the facilitation and assistance of CCTV technology. For

[28] See Guidance Note, page 1.

example, it may not be able to monitor and prevent an accident from happening and may not be able to uncover the cause of a fatal accident in its post incident investigation.

4.9 "Adequacy" and "appropriateness" but "not excessive" were used as yardsticks for the assessment of the personal data system by installation and use of CCTVs during onsite inspections. In the interviews with Station Controllers, they were able to demonstrate and illustrate the following :-

4.9.1 In Central Station, the CCTVs installed and used at Entrance / Exit A, next to the Worldwide House Shopping Arcade, were considered particularly useful for the prevention of crowds from blocking the entrance / exit on Sundays and public holidays;

4.9.2 The CCTVs installed and used at the passenger drop-off areas in the Hong Kong Station (Photo 14) and Tuen Mun Station were also considered very useful in facilitating the station controllers in making staff deployment decisions, for example, to assist passengers on wheelchairs and other needed passengers;

4.9.3 The CCTVs installed and used at the Public Transport Interchange outside the Tuen Mun Station (Photo 15) were considered very useful in crowd and traffic control, especially in the deployment of shuttle buses for the transfer of passengers overflowed from the broken down West Rail service; and

Photo 14

A camera installed at the passenger drop-off areas in Hong Kong Station.

Photo 15

A camera installed at the Public Transport Interchange outside the Tuen Mun Station.

4.9.4 As there is no train captain in the Disneyland Resort Line, the installation and use of CCTVs in the train captain's cabin as a remote train captain were significant and vital to the System Controller, who works at the Sunny Bay Station.

4.10 Although there are obviously less privacy intrusive alternatives, the installation and use of CCTVs in the circumstances is justisfied for the discharge of MTR's statutory and contractual obligations were justified as the performance of MTR's lawful functions and activities.

Has any assessment been conducted ?

4.11 As suggested in the Guidance Note, "*An organization should conduct an assessment objectively before installing CCTV to ensure that it is the right response to tackle the existing problem…and is proportionate to the degree of intrusion into personal data privacy in addressing the problem*". The Inspection revealed that MTR has not conducted such assessment on their CCTV system.

4.12 In considering whether to install and use CCTV, a PIA[29] or similar

[29] Information Leaflet : Privacy Impact Assessments (PIA) issued by PCPD in July 2010.

assessment covering the following steps should be conducted :-

4.12.1 Decide whether there is a pressing need to use CCTV;

4.12.2 Establish a specific purpose of the use of CCTV and clearly identify the problem to be addressed;

4.12.3 Collect relevant information to see whether CCTV will substantially solve the existing problem;

4.12.4 Find out whether there are other options that could better address the problem than using CCTV or that could be used together with CCTV to make it more effective or less privacy intrusive;

4.12.5 Consult where practicable people who may be affected by the CCTV. What will be the concerns of those under surveillance? What steps can be taken to minimize the privacy intrusion and address the concerns of these people?

4.12.6 Clearly determine the scope or extent of monitoring.

4.13 Although MTR answered most of the questions above, it had not conducted a systematic privacy risk assessment that should have been integrated into their decision making process. One may argue that even if MTR had conducted a PIA, it would have arrived at the same result and conclusion. However, conducting a PIA means that the data processing cycle and privacy risks would have been identified and analyzed. Measures could then be put in place for minimizing such risks. The PIA process also enables the MTR decision maker to adequately consider the impact on personal data privacy; directly address the privacy problems identified in the process by solutions and safeguards; provides benchmarks for future privacy compliance audit and control; and most important of all, provides a credible source of information to allay any privacy concerns from the public and the stakeholders.

Where are the CCTVs and notices positioned ?

4.14 CCTV cameras should be positioned in a way that will not unnecessarily intrude into the privacy of individuals. No CCTV cameras should be used in places where people have a reason to expect privacy. People should be explicitly informed by conspicuous notices at the entrance to the monitored area that they are subject to CCTV surveillance and reinforced by fixing further notices inside the area. The notices should contain details of

the organization operating the CCTV system, the specific purpose of monitoring and the person to whom matters relating to personal data privacy issues can be raised.

4.15 The Team found during the onsite inspections that all CCTV cameras used in both the public areas of station premises and train compartments are overtly installed and visible to commuters.

4.16 Many CCTV cameras installed and used in the public areas, especially at entrances and exits, of the station premises are pan-tilt-zoom and can capture images of non-users and areas adjacent to the station premises. For example, the CCTV camera at the MTR entrance, and exit at Hennessy Road would often be used to monitor the public procession on Hennessy Road for the purpose of station crowd and traffic control; the CCTV camera at Customer Services Centre may also be used to monitor money transaction or cash in transit at Central Station. However, onsite inspection revealed that these CCTV cameras have been set to a pre-determined default position, i.e. the entrance or exit or its originally intended position. Whenever these CCTV cameras are used for monitoring the adjacent or other areas, the last action of the CCTV operators is to always return the CCTV camera to the default position of not intruding unnecessarily into the privacy of individuals. By adjusting the camera back to its default position of pointing at locations within premises and to an angle not pointing at any fixed location, unnecessary intrusion and personal data collection can be minimized.

4.17 During the onsite inspection, no CCTV was found capturing images of restrooms in stations. CCTVs in Kowloon Tong, Mei Foo, Disneyland Resort Line and Tai Wai stations were also thoroughly reviewed and were found to be incapable of capturing images inside restrooms.

4.18 MTR displays CCTV-in-operation notices prominently and conspicuously in train compartments close to the location of the CCTVs. However, MTR displays CCTV-in-operation notices neither prominently nor conspicuously: at entrances to the station premises together with other notices; in the "*Travel Safely Everyday in the MTR*" booklet together with other information; and close to the location of CCTVs in the public areas of station premises. The notices at the drop off point at the Tuen Mun Station and the Central Station (Photos 16 and 17) were not standard notices regularly used by

MTR. All notices did not contain sufficient information; they did not include the officer to whom matters relating to personal data privacy issues can be raised, etc. Although it is appreciated that with the great number of CCTV cameras installed and used, MTR users should not be bombarded with a vast number of notices, consideration should be given to the sufficiency, visibility and content of the notices to ensure they are prominent, conspicuous and contain the necessary details. The "*Travel Safely Everyday in the MTR*" booklet might be reviewed and revised to provide sufficient information in.

Photo 16

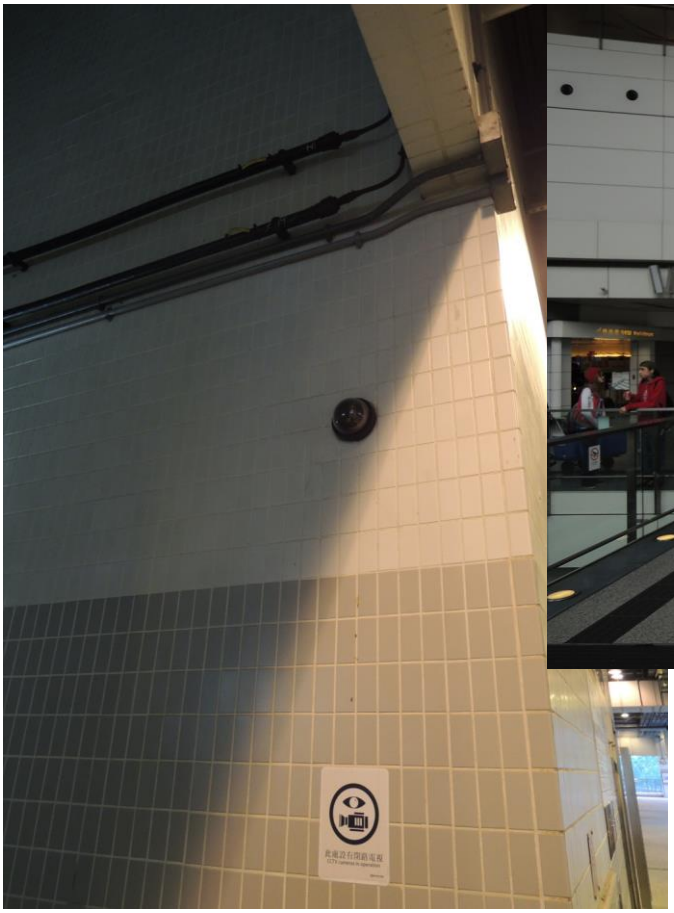

Photo 17

The notices at the drop off point at the Tuen Mun Station and the Central Station were not standard notices regularly used by MTR.

Stage 2: Recording and Storage

Are the recorded images handled properly ?

4.19 **DPP2** imposes a duty on data users to ensure data accuracy and that there is no excessive retention of personal data. The personal data collected should be deleted from the CCTV as soon as practicable once the purpose of collection is fulfilled.

4.20 The digital video image captured by MTR's CCTV is encrypted and recorded in the hard disk of a DVR system. Recorded images in the DVR hard disk will automatically be overwritten by new recorded images upon expiry of the retention period and recorded images on the VCR tape will automatically be overwritten on the re-cycled and serially-numbered VCR tape by the newly recorded images. However, during the site inspection on 12 December 2012 to the Sunny Bay Station, the Team was able to retrieve digital CCTV images of Disneyland Resort Line recorded on 1 November 2012 when the retention period laid-down was 10 days only.

4.21 As recorded images may be retrieved, used and transferred, digital and analogue copies may in the process be created and stored. However, there was no policy or procedure on how these recordings and copies should be destroyed or erased. These processes had only been done at random at the discretion of individual officers. The Team found in the site inspection of the HQ of MTR that there is no regular exercise or formal record of purging CCTV records kept by Operations Safety Section. MTR should therefore consider improving the enforcement of its retention and storage rules.

4.22 The CCTV retention periods have been well determined and stated clearly in the MTR's Administration Manual. However, the periods vary from 5 days to 28 days for 11 rail lines and differ between recordings made by the analogue and digital CCTV systems. The different retention periods and related management systems should be rationalized and aligned.

4.23 **DPP4** requires data users to take all reasonably practicable steps to ensure that the personal data held by them is protected against unauthorized or accidental access, processing, erasure, loss or other use.

4.24 For physical protection, security measures must be in place to prevent unauthorized access to the CCTV system. Recorded images should be kept in safe custody. Proper records of the staff members taking charge of and keeping the recorded images should be maintained. Transfers and movements of the recorded images should also be clearly documented. For electronic documents, the hard disks or any devices storing the recorded images should be securely protected from unauthorized access and only viewed, retrieved or handled upon proper authorization for the intended purpose. Once the reasons for retaining the recorded images no longer applies, they should be deleted. There must be sufficient safeguards in place to protect wireless transmission systems from interception. The access to places where the images recorded by the CCTV cameras are viewed, stored or handled should be secured and restricted to authorized persons only.

4.25 The computer system that stores these CCTV video footages is password protected and can only be accessed by authorized staff members. The room where such computer system is placed is locked and the cabinets storing the CCTV footages are always secured. Access to the CCTV footages is restricted to authorized persons only. However, the computer login account and password for accessing the computer recording and storing CCTV footages for the Island Line, Kwun Tong Line, Tsuen Wan Line, Tseung Kwan O Line, Airport Express Line, Tung Chung Line, Disneyland Resort Line and Heavy Rail stations in the Operations Safety Section's AV Room on 15/F of the HQ CCTV room was shared among five staff members working in the Operations Safety Section. Although this password sharing arrangement has not given rise to any data leakage issue, the practice is prone to data leakage and will become a contentious point as user accountability cannot be enforced.

4.26 It was noted in the Inspection that CCTV footages taken in trains of the Disneyland Resort Line is transmitted using wireless local area network (commonly known as Wi-Fi or WLAN) technology. During the on-site inspection, the information provided by MTR concerning the security measures of WLAN could not be ascertained as the MTR-designated interviewees were not suitably qualified in information technology. In view of this, the Team sent a post-inspection inquiry to MTR to seek clarification in writing as to the precise security measures adopted.

4.27 MTR subsequently represented to the Team that "*the wireless LAN based on IEEE 802.11a is password protected. The communication is based on 5.8GHz band and TCP/IP [Transmission Control Protocol/Internet Protocol] standards to ensure system safety against external interception. The network is only accessible to registered wireless device, and device authentication is provided by Mobile Internet Service Protocol, it cannot be accessed by non-registered mobile router and cannot be tapped by ordinary AP [Access Point]. The data is encrypted and protected by AES [Advanced Encryption Standard]…The reliability and data security confirms to that of IEEE 802.11a standard. In addition, video files are in a special format that can only be played back with the proprietary player [omitted for security reasons]".*

4.28 As all this explanation took place after the on-site inspection and was received only shortly before conclusion of the report, the Team was unable to further verify the WLAN security measures noted in the reply, such as why the communication standards of IEEE 802.11a, 5.8GHz frequency band and TCP/IP were relevant to security protection. Therefore, the Team is unable to draw a conclusion on whether MTR has taken all reasonably practicable steps to ensure the compliance of DPP4 in relation to the wireless transmission of the data.

4.29 Demonstration of the system by the MTR staff and observations of the Team during the Inspection revealed that CCTVs were viewed and retrieved according to date, time, location and the approving authority rather than by the identity of the individual making the request. Control room facilities, access card control, visitors' log, password control to the Station Controllers' desktop, DVR system, DVR system password control, access right and encryption, VCR system, locked cabinets storing VCR tapes, key movements, in train footages and hard disk storage were examined and no irregularities were identified. This finding supported the result of interviews with MTR staff and MTR's representations. However, the password sharing practice at the Operations Safety Section's AV Room and the disparity in CCTV record retention periods call for further improvement.

Stage 3: Retrieval, Use and Transfer

How are CCTV records transferred to third parties ?

4.30 **DPP3** provides that personal data shall only be used for the purposes for which they were collected or a directly related purpose, unless the data subject gives prescribed consent or when any applicable exemptions under the Ordinance apply.

4.31 When a data user is asked to provide copies of CCTV records to a law enforcement agency for criminal investigation purpose, the provisions of section 58 of the Ordinance may apply. However, a data user should exercise due care when relying on the exemption under section 58(2) of the Ordinance in disclosing personal data to third parties. Data users may disclose the CCTV records to third parties after satisfying themselves that the use of the data is exempted.

4.32 At the MTR, generally speaking all requests for viewing of CCTV footages must be made to the OSaM for consent before any viewing can be arranged, not to mention copying and transferring of the footages. Where a request for CCTV footage is made by the Court Liaison Office, or an external law firm for the purposes of legal proceedings or prosecution, such request will be referred to the MTR legal department for screening on a case by case basis before routing through to the OSaM for consideration. Even though a request for viewing may be approved, the CCTV viewing still has to be conducted at designated places or with designated CCTV player. If there is any reproduction of the CCTV images, a proper record of the reproduction and / or leasing of the copy has to be kept and maintained by the OSaM. The Team found from the relevant files at MTR HQ that MTR also reminds requesters in their correspondences with them that "*we now send you a copy of the CCTV record subject to the condition that you shall not use the CCTV record for any other purpose*". As MTR was observed to have been using personal data for the purposes directly related to its collection purposes or relying on the exemption under section 58(2) of the Ordinance with due care and vigilance, the Team found MTR to be DPP3-compliant.

Other Findings on the Personal Data Flow

Personal Information Collection Statement

4.33 Although the personal data of MTR passengers and others would be collected, recorded, stored, retrieved, used and transferred to third parties, no PICS to this effect had been given to the MTR passengers and others. In addition to the PICS on the MTR website[30], consideration should be given to revise and improve the "*Travel Safely Everyday in the MTR*" booklet, the MTR website and the MTR notices at entrances and exits to station premises, etc. so that MTR passengers and others would be better informed of the MTR's PICS.

Use of USB thumb drive

4.34 At the Kowloon Tong Station, CCTV images and footages of the East Rail Line are stored and can only be retrieved and copied in a satellite control room, which used to be the former Kowloon and Canton Railway Corporation Kowloon Tong station control room before amalgamation with MTR. In case there is a request for CCTV record of the East Rail Line, the recorded images have to be copied to a USB thumb drive in the satellite control room, carried to and copied to CD / DVD disk in the Kowloon Tong station control room, which has always been the MTR station control room. It was found in the Inspection that the USB thumb drive was not encrypted, contrary to MTR's Security Policy for Mobile Computing Devices. Although the USB thumb drive is one of the items for handing over by the shift station controllers when they come on/off duty, the copying and transferring of CCTV recorded images by using a USB thumb drive without encryption is unsatisfactory. Improvement in the above area is clearly called for.

Privacy Policy and Practice

4.35 **DPP5** requires data users to make generally available their privacy policy and practice.

4.36 CCTV monitoring policies and procedures should be devised to

[30] http://www.mtr.com.hk/chi/legal/cust_privacy.html.

ensure that matters such as the kinds of personal data held, the main purposes for which the data collected is to be used and the retention policies are clearly set out and communicated to the data subjects. It is important to establish who has the responsibility of operating the CCTV system and for the control of the zoom-in functions and to decide what are to be recorded, how the recorded images should be used and to whom they may be disclosed. It is also necessary to ensure that the policies or procedures are communicated to and followed by the relevant staff members. Staff who operate the systems or use the images should be trained to comply with the policies or procedures. Adequate supervision should also be in place. Misuse or abuse of the CCTV system or the recorded images should be reported to a senior member of the staff and appropriate follow up actions, including disciplinary action, can be taken.

4.37 MTR provided the following policy / procedural documents in relation to personal data protection for the Inspection. The documents are posted on MTR's Intranet and / or on display at prominent areas of stations :-

MTR Reference	Name of Documents	Available at
	Personal Data Privacy Compliance Manual	Intranet
	MTR Administration Manual	Intranet and stations
CGI213	Information Management Corporate Policy	Intranet
CGI241	Protection of Classified Corporation Information	Intranet
CGI270	Security Policy for Mobile Computing Devices	Intranet
CGI291	Corporate Policy on Personal Data (Privacy)	Intranet

4.37.1 ***Personal Data Privacy Compliance Manual*** sets out how MTR shall comply with the Ordinance;

4.37.2 ***The MTR Administration Manual*** includes the appendices on the "*1A4.3 CCTV Recording System*", which governs the collection, recording, storage, retrieval, use and transfer of CCTV footages in operation;

4.37.3 ***CGI 213 on Information Management Corporate Policy*** sets out MTR's corporate policy on information

management, including protection of classified information, protection of personal data privacy, etc.;

4.37.4 ***CGI241 on the Protection of Classified Corporation Information*** sets out the rules on classification of information and how classified information should be protected;

4.37.5 ***CGI 270 on Security Policy for Mobile Computing Devices*** relates to security policy for mobile computing devices, e.g. USB thumb drives and external hard disks; and

4.37.6 ***CGI 291 on Corporate Policy on Personal Data (Privacy)*** is an update to MTR's policy having regard to the Ordinance and "recent development"[31] .

4.38 Onsite inspection and interview with MTR staff revealed that :-

4.38.1 MTR staff are generally conversant with their internal policies and procedures;

4.38.2 They know that CCTV footages are classified as "Restricted" documents and the related procedures for handling them;

4.38.3 They know that they may not capture CCTV images by the use of their own mobile devices;

4.38.4 They have general awareness of privacy issues and realize the importance of returning the CCTV cameras to the default position after adjusting it to monitor other locations;

4.38.5 Station controllers do not entertain requests for viewing CCTV footage from individuals;

4.38.6 Administration Manual is available in every station control room and so does the CGIs;

4.38.7 Station Controllers of one of the stations inspected have difficulty in retrieving the "Personal Data Privacy Compliance Manual" from the MTR's intranet; and

4.38.8 Hardcopy of CGI is displayed in stations and offices. Soft

[31] Quoted from CGI 291.

copy of CGI is also available and accessible to all staff with an account through the intranet.

Conclusion

4.39 Having conducted an inspection pursuant to section 36 of the Ordinance on the MTR personal data system with respect to the installation and use of CCTV, the Team identified the following issues of importance :-

4.39.1 no assessment or PIA was conducted or reported;

4.39.2 CCTV notices were insufficient, inadequate and sub-standard in terms of both quantity and quality;

4.39.3 no policy and procedures to explain how CCTV recorded images copies should be destroyed or erased;

4.39.4 no control on retention and storage periods;

4.39.5 disparity of retention periods and management systems between different lines and systems;

4.39.6 sharing of login account and password of the DVR System by the Operations Safety Section;

4.39.7 use of USB thumb drive without encryption for copying, storage and transfer of CCTV personal data; and

4.39.8 personal data privacy related policies and procedures were found in many different kinds of internal manuals.

4.40 As the Team did not have the opportunity to discuss with suitably qualified MTR staff on many IT protection measures deployed by MTR on the transmission and storage of CCTV footages during the on-site inspection period, the Team had to rely on the assertions provided by MTR on such measures. The Team could not therefore rule out there could be other issues of importance in this respect.

4.41 As the largest public transport operator in Hong Kong, the experience and assessment of the MTR personal data system may shed light on the use of personal data system by other public transport operators and demonstrate how personal data privacy intrusion, if any, can be minimized and overcome.

Recommendation

4.42 In furtherance of the conclusion drawn above, the following recommendations are made :-

4.42.1 A PIA should be conducted to help identify and address potential privacy issues;

4.42.2 Consideration should be given to the visibility and sufficiency of the CCTV notices and the information therein to ensure they are more prominently and conspicuously displayed with all the necessary details;

4.42.3 The "*Travel Safely Everyday in the MTR*" booklet should be reviewed and refined to provide more information on the CCTV system;

4.42.4 The PICS contained in "*Travel Safely Everyday in the MTR*" booklet, and on the MTR website and MTR notices at entrances and exits to station premises, should be reviewed and refined so that MTR passengers can be better informed of the PICS;

4.42.5 Policy and procedures on the erasure of CCTV records or copy CCTV records should be formulated and carried out by fully trained staff who are conversant with the procedures;

4.42.6 Access to computer recording and storage of CCTV footages should not be shared to ensure accountability and data security;

4.42.7 Policy and procedures on the use of portable storage devices (e.g. USB thumb drive) should be enforced to prevent possible unauthorized access or loss of CCTV footage in transit; and

4.42.8 Consideration should be given to streamline and consolidate all data privacy policies and procedures, instructions and guidelines, and to review or align the disparity between CCTV retention periods of CCTV records among different railway lines. This will promote compliance and user-friendliness and to facilitate training and.

Annex 1 - Data Protection Principles

1. **Principle 1-purpose and manner of collection of personal data**

(1) Personal data shall not be collected unless-

(a) the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
(c) the data is adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are-

(a) lawful; and
(b) fair in the circumstances of the case.

(3) Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that-

(a) he is explicitly or implicitly informed, on or before collecting the data, of-
  (i) whether it is obligatory or voluntary for him to supply the data; and
  (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
(b) he is explicitly informed-
  (i) on or before collecting the data, of-
    (A) the purpose (in general or specific terms) for which the data is to be used; and
    (B) the classes of persons to whom the data may be transferred; and
  (ii) on or before first use of the data for the purpose for which it was collected, of-
    (A) his rights to request access to and to request the correction of the data; and
    (B) the name or job title, and address, of the individual who is to

handle any such request made to the data user,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data is exempt from the provisions of data protection principle 6.

2. **Principle 2-accuracy and duration of retention of personal data**

(1) All practicable steps shall be taken to ensure that-

(a) personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used;

(b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used-

(i) the data is not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data is erased;

(c) where it is practicable in all the circumstances of the case to know that-

(i) personal data disclosed on or after the appointed day to a third party is materially inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used by the third party; and

(ii) that data was inaccurate at the time of such disclosure,

that the third party-

(A) is informed that the data is inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used.

(3) Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to

prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

(4) In subsection (3)—

data processor (資料處理者) means a person who—

(a) processes personal data on behalf of another person; and

(b) does not process the data for any of the person's own purposes.

3. Principle 3-use of personal data

(1) Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose.

(2) A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his or her personal data for a new purpose if—

(a) the data subject is—

(i) a minor;

(ii) incapable of managing his or her own affairs; or

(iii) mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap 136);

(b) the data subject is incapable of understanding the new purpose and deciding whether to give the prescribed consent; and

(c) the relevant person has reasonable grounds for believing that the use of the data for the new purpose is clearly in the interest of the data subject.

(3) A data user must not use the personal data of a data subject for a new purpose even if the prescribed consent for so using that data has been given under subsection (2) by a relevant person, unless the data user has reasonable grounds for believing that the use of that data for the new purpose is clearly in the interest of the data subject.

(4) In this section—

new purpose (新目的), in relation to the use of personal data, means any purpose other than—

(a) the purpose for which the data was to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a).

4. **Principle 4-security of personal data**

(1) All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to-

(a) the kind of data and the harm that could result if any of those things should occur;
(b) the physical location where the data is stored;
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;
(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
(e) any measures taken for ensuring the secure transmission of the data.

(2) Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

(3) In subsection (2)—
data processor (資料處理者) has the same meaning given by subsection (4) of data protection principle 2.

5. **Principle 5-information to be generally available**

All practicable steps shall be taken to ensure that a person can-

(a) ascertain a data user's policies and practices in relation to personal data;
(b) be informed of the kind of personal data held by a data user;
(c) be informed of the main purposes for which personal data held by a data user is or is to be used.

6. **Principle 6-access to personal data**

A data subject shall be entitled to-

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data-

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

Annex 2- Guidance on CCTV Surveillance Practices

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Guidance Note

Guidance on CCTV Surveillance Practices

Introduction

The use of CCTV[1] in public places or common areas of buildings for security reasons or for monitoring illegal acts[2] (e.g. throwing objects from a height) has become increasingly widespread. However, since CCTV may capture extensive images of individuals or information relating to individuals, any indiscriminate use of CCTV inevitably involves intrusion into the privacy of individuals.

This guidance note offers advice to organizations on whether CCTV should be used and how to use CCTV responsibly and to help them to understand some of the requirements under the Personal Data (Privacy) Ordinance (the "Ordinance") relating to the collection of personal data.

In relation to the use of CCTV to monitor and record employees' activities at workplaces, guidance can be found in the "Privacy Guidelines: Monitoring and Personal Data Privacy at Work" issued by the Privacy Commissioner for Personal Data.

Is it necessary to use CCTV?

Data Protection Principle ("DPP") 1(1) of the Ordinance requires that personal data shall only be collected where it is necessary for a lawful purpose directly related to the function or activity of the data user and that the data collected shall be adequate but not excessive.

In assessing whether it is necessary to use CCTV, the prime question to ask is –

"Is the use of CCTV in the circumstances of the case justified for the performance of the lawful function and activity of the organization and whether there are less privacy intrusive alternatives?"

Take for example, while the use of CCTV for deterring and detecting criminal activities like the throwing of corrosive liquid from a height appears to be justifiable, the use of CCTV inside taxi for general security reason may be regarded as privacy intrusive. For the purpose of crime prevention, due consideration should be given to the use of less privacy intrusive alternatives that could achieve the same purpose.

To conduct an assessment before installation

An organization should conduct an assessment objectively before installing CCTV to ensure that it is the right response to tackle the existing problem (e.g. the throwing of objects from a height) and is proportionate to the degree of intrusion into personal data privacy in addressing the problem. In considering whether to install CCTV, the following steps should be taken:

- Decide whether there is a pressing need to use CCTV (for example, if the use involves public interest).
- Establish a specific purpose of the use of CCTV and clearly identify the problem to be addressed. For example, a bank may intend to use CCTV to monitor the unlawful activities happening in the vicinity of the ATM machines and the operator of a public car park may intend to use CCTV to monitor the security of visitors and the vehicles parked.
- Collect relevant information to see whether CCTV will substantially solve the existing problem. For example, if a property management body intends to use CCTV to

[1] "Closed Circuit Television" - camera surveillance systems or other similar surveillance devices that capture images of individuals.

[2] Covert surveillance conducted by a law enforcement agency is regulated by the Interception of Communications and Surveillance Ordinance, Cap 589.

tackle the problem of objects thrown from a height, any statistics of similar event happening and the effectiveness of the use of CCTV to successfully prevent or detect the incident may be relevant.

- Find out whether there are other options that could address the problem better than using CCTV or that could be used together with CCTV to make it more effective or less privacy intrusive.

- Consult where practicable people who may be affected by the CCTV. What will be the concerns of those under surveillance? What steps can be taken to minimize the privacy intrusion and address the concerns of these people?

- Clearly determine the scope or extent of monitoring. It is not appropriate to use CCTV permanently when it is intended to address a temporary need.

Positioning of CCTV cameras and notices

CCTV cameras should be positioned in a way that will not unnecessarily intrude into the privacy of individuals. No CCTV cameras should be placed in places where people have a reason to expect privacy (e.g. changing room). The CCTV system as a whole should be properly protected from vandalism or unlawful appropriation.

Only when there is an actual need, such as for identification purpose in criminal trials will the use of high quality equipment to record individuals' detailed facial images be justified. Detailed facial images are generally not required when CCTV is used for monitoring the flow of traffic or movement of crowd.

People should be explicitly informed that they are subject to CCTV surveillance. An effective way is to put conspicuous notices at the entrance to the monitored area and reinforced by fixing further notices inside the area. It is particularly important where the CCTV cameras themselves are very discreetly located, or places where people may not expect to be subject to surveillance.

The notices should contain details of the organization operating the CCTV system, the specific purpose of monitoring and the person to whom matters relating to personal data privacy issues can be raised.

Proper handling of the recorded images

DPP2 imposes a duty on data users to ensure data accuracy and that there is no excessive retention of personal data.

The personal data collected should be deleted from the CCTV as soon as practicable once the purpose of collection is fulfilled. For instance, the recorded images captured by the CCTV installed for security purpose should be safely deleted regularly when no incident of security concern is detected or reported.

DPP4 requires data users to take all reasonably practicable steps to ensure that the personal data held by them are protected against unauthorized or accidental access, processing, erasure or other use.

Security measures must be in place to prevent unauthorized access to the CCTV system. Recorded images should be kept in safe custody. Proper records of the staff members taking charge of and keeping the recorded images should be maintained. Transfers and movements of the recorded images should also be clearly documented.

To manage the risk posed by the advancement in technology, the hard disks or any devices storing the recorded images should be securely protected from unauthorized access and only viewed, retrieved or handled upon proper authorization for the intended purpose. Once there is no valid reason to retain the recorded images, they should be deleted.

There must be sufficient safeguards in place to protect wireless transmission systems from interception. The access to places where the images recorded by the CCTV cameras are viewed, stored or handled should be secured and restricted to authorized persons only.

Transfer of CCTV records to third parties

On the use of personal data, **DPP3** provides that personal data shall only be used for the purposes for which they were collected or a directly related purpose, unless the data subject gives prescribed

consent (meaning express consent given voluntarily) or when any applicable exemptions under the Ordinance apply.

When a data user, e.g. building management company, is asked to provide copies of CCTV records to a law enforcement agency, e.g. Police, for criminal investigation purpose, the provisions of section 58 of the Ordinance[3] may apply.

However, a data user should exercise due care when relying on the exemption under section 58(2) of the Ordinance in disclosing personal data to third parties (including the Police). If the information is disclosed on a ground that is not lawfully recognized, serious harm may be caused to data subject's personal data privacy. The organization using the CCTV should not disclose the CCTV records by just relying on the words of or general allegation made by the requestor. Data users may disclose the CCTV records to third parties upon sufficient information to satisfy themselves that the use of the data are exempted, e.g. under section 58 of the Ordinance.

Transparency of policy and practice

DPP5 requires data users to make generally available their privacy policy and practice.

Organizations should devise CCTV monitoring policies and/or procedures to ensure that matters such as the kinds of personal data held, the main purposes for which the data collected are to be used and the retention policies are clearly set out and communicated to the data subjects.

It is also important to establish who has the responsibility of operating the CCTV system and for the control of the zoom-in functions (if any), and to decide what are to be recorded, how the recorded images should be used and to whom they may be disclosed.

It is necessary to ensure that the policies or procedures are communicated to and followed by the relevant staff members. Staff who operate the systems or use the images should be trained to comply with the policies or procedures. Adequate supervision should also be in place. Misuse or abuse of the CCTV system or the recorded images should be reported to a senior member of the staff and appropriate follow up actions, including disciplinary action, can be taken.

Regular reviews

Compliance checks and audits have to be carried out regularly by the organizations to review the effectiveness of the safeguards and procedures for the CCTV system.

The need to use CCTV which are in existence should be reviewed regularly to ensure that they are serving the purpose for which they were installed. If such reviews indicate that the use of the CCTV is not or is no longer necessary or when less privacy intrusive alternatives can be used to achieve the same purpose, the organization should cease using the CCTV.

[3] A data user may rely on the exemption under section 58(2) of the Ordinance to exempt from the provisions of DPP3 on the use of personal data for the prevention or detection of crime.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Enquiry Hotline: (852) 2827 2827
Fax: (852) 2877 7026
Address: 12/F, 248 Queen's Road East, Wanchai, Hong Kong
Website: www.pcpd.org.hk
Email: enquiry@pcpd.org.hk

Annex 3- Sample of CCTV notices

(1) CCTV notices at entrances / exits

Actual Size: 388 (Width) x 518 (Height) mm

(2) CCTV notices at train compartments

Actual Size: 150 (Width) x 200 (Height) mm

(3) CCTV notices at Light Rail stations

Actual Size: 360 (Width) x 132 (Height) mm