For information

Legislative Council Panel on Transport
Installation of Camera Systems inside Taxi Compartments

Purpose

This paper is prepared upon Members' request to brief them on matters relating to the installation of camera systems inside taxi compartments by the taxi trade.

Background

2. The Government has noted that the Association for Taxi Industry Development ("the Association"), which is formed by some members of the taxi trade, proposed to install camera systems inside some taxi compartments on a trial basis in order to strengthen the monitoring of drivers' service and minimise disputes between drivers and passengers. According to the information provided by the Association, there are currently around 40 taxis participating in the trial scheme. Labels indicating camera-in-operation have been affixed onto the conspicuous place of these taxi bodies, and drivers will orally remind passengers of the operation of the camera systems. The Association said that the video footage recorded will be encrypted and will only be decrypted upon request by the Police or passengers to avoid drivers from using or tampering with the footage. It is learnt that the Association aims to install the camera systems inside about 2 000 taxis in the coming year.

Privacy issues

3. Taxis provide personalised point-to-point transport service and only the driver and passenger(s) are inside the compartment. If there is dispute between the passenger(s) and the driver over the service issue, it is often difficult to follow up on the case in the absence of witnesses to provide evidence.

4. The community in general calls for improvement of the service quality of taxis. The Government welcomes the trade to initiate various measures to improve their service quality, but the pre-requisite is

that such measures shall comply with the current legal requirements and provisions before they can be implemented.

5. In general, application to the Transport Department for installing camera systems inside taxi compartments is not required if it does not affect the vehicle structure and driving safety. However, the Government has noted that the installation of such camera systems will involve the problem of privacy protection. Some members of the public have concerns on installing camera systems inside taxi compartments and are worried that the personal data privacy cannot be fully protected.

6. The Government has enquired with the Office of the Privacy Commissioner for Personal Data ("PCPD") on whether the trial scheme would give rise to the problem that the personal data privacy cannot be fully protected. According to PCPD, Personal Data (Privacy) Ordinance ("Ordinance") at present does not prohibit any individual or organisation from installing or using closed circuit televisions ("CCTV"), or require the consent of PCPD prior to any such installation or use. However, the Ordinance stipulates that any person (i.e. data users), who controls the collection, holding, processing or use (including disclosure and transfer) of the personal data, shall comply with the requirements under the Ordinance, including the six Data Protection Principles (see **Annex 1** for details). PCPD considers that the installation of cameras inside taxi compartments to record images and sounds of passengers is by nature intrusive to privacy to a certain extent. Hence, there should be detailed consideration and assessment on whether the installation is necessary for a lawful purpose (such as enhancing service quality or preventing crimes), whether it is proportionate to the gravity of the prevailing problems (such as overcharging), as well as balancing of the interests and safety of drivers and passengers, prior to the implementation of the trial scheme. PCPD has published the Guidance on CCTV Surveillance and Use of Drones to provide organisations with suggestions on whether and how to properly use CCTV in order to assist individuals or organisations in complying with the requirements of the Ordinance (see **Annex 2** for details). The above guidance is applicable to the installation of camera systems inside taxi compartments. As at 5 December 2016, PCPD has not received any complaint relating to the installation of camera systems inside taxi compartments. PCPD will continue to liaise closely with different stakeholders, keep in view development of the matter, and take appropriate follow-up as necessary.

7. If necessary, TD is willing to assist the trade in keeping communication with PCPD. The Department will also keep close

communication with the trade on the implementation progress of the trial scheme, as well as closely monitor the public opinion on the matter.

Transport and Housing Bureau
6 December 2016

[sections 2(1) & (6)]

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- (Amended 18 of 2012 s. 40)

(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- (Amended 18 of 2012 s. 40)

(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, (Replaced 18 of 2012 s. 40)

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.

(Amended 18 of 2012 s. 40)

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- (Amended 18 of 2012 s. 40)

(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. (Amended 18 of 2012 s. 40)

(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. (Amended

18 of 2012 s. 40)
(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. (Added 18 of 2012 s. 40)
(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. (Added 18 of 2012 s. 40)

(Amended 18 of 2012 s. 40)

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. (Amended 18 of 2012 s. 40)
(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. (Added 18 of 2012 s. 40)
(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. (Added 18 of 2012 s. 40)
(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). (Added 18 of 2012 s. 40)

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- (Amended 18 of 2012 s. 40)
(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; (Amended 18 of 2012 s. 40)
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored; (Amended 18 of 2012 s. 40)
(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. (Added 18 of 2012 s. 40)
(3) In subsection (2)—
data processor (資料處理者) has the same meaning given by subsection (4) of data protection principle 2. (Added 18 of 2012 s. 40)

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. (Amended 18 of 2012 s. 40)

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).

(Enacted 1995)

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 and Use of Drones

INTRODUCTION

The use of CCTV[1] covering public places or common areas of buildings for security reasons or for monitoring illegal acts[2] (e.g. throwing objects from heights) has become increasingly widespread. Since CCTV may capture extensive images of individuals or information relating to individuals, its use should be properly controlled to avoid intrusion into the privacy of individuals.

This guidance note offers advice to data users (both organisational and individual data users) on determining whether CCTV should be used in given circumstances and how to use CCTV responsibly. Owing to the increased popularity of unmanned aircraft systems (more commonly known as "**Drones**") for use in photography, surveying and surveillance, the latter part of this guidance note also provides recommendations on the use of drones from the perspective of protecting personal data privacy.

Recommendations given in this guidance note are based on the key requirements under the Personal Data (Privacy) Ordinance (the "**Ordinance**") relating to the collection of personal data.

As regards the use of CCTV to monitor and record employees' activities at workplaces, more specific guidance can be found in "Privacy Guidelines: Monitoring and Personal Data Privacy at Work"[3] issued by the Privacy Commissioner for Personal Data (the "**Commissioner**").

CCTV

Privacy Impact Assessment for CCTV Installation

Before using CCTV, data users should carry out a privacy impact assessment, taking into account at least the following factors:

- **Assessment** – Are the design and use of the CCTV system appropriate, necessary and proportionate for the given circumstances?
- **Alternatives** – Are there other less privacy intrusive means than the use of CCTV to achieve the same objective?
- **Accountability** – Has the data user acted and been seen to have acted responsibly and transparently, in terms of its policy, controls, and compliance with the Ordinance, in the use of CCTV?

1 "Closed Circuit Television" – camera surveillance systems or other similar surveillance devices that are capable of capturing images of individuals.
2 Covert surveillance conducted by a law enforcement agency is regulated by the Interception of Communications and Surveillance Ordinance, Cap 589.
3 See www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/monguide_e.pdf

CCTV and the Ordinance

If a CCTV system does not have recording function (still pictures or video), its use will normally not involve collection of personal data as defined under the Ordinance, and is therefore not regulated under the Ordinance.

On the other hand, whether the domestic or personal use of CCTV systems covering semi-public/public areas (such as surveillance cameras installed outside a residential unit or dash cams inside vehicles) is regulated by the Ordinance would depend on whether the purpose of the installation is to collect or compile information about identified persons.

If employers of domestic helpers use CCTV systems to monitor their helpers, they should read "Monitoring and Personal Data Privacy at Work: Points to Note for Employers of Domestic Helpers"[4] issued by the Commissioner.

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 primary 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 data user and whether there are less privacy intrusive alternatives?"

For example, the use of CCTV for deterring and detecting specific or repeated criminal activities like the throwing of corrosive liquid from heights would appear to be justifiable. In any case, for the purpose of crime prevention, due consideration should be given to the use of less privacy intrusive arrangements or alternatives that could achieve the same purpose.

A data user should conduct an assessment objectively before installing CCTV to ensure that it is the right response to tackle the problem at hand (e.g. the throwing of objects from heights) and the degree of intrusion into privacy is proportionate to the severity of the problem. The following steps should be taken:

- Decide whether there is a pressing need to use CCTV (for example, if the use involves public interest or public safety);
- Find out whether there are other less privacy intrusive options to better address the problem or that could be used together with CCTV to make it more effective or less privacy intrusive;
- Establish the specific purpose of the use of CCTV and clearly identify the problem to be addressed. For example, a bank may want to use CCTV to deter thieves from robbing customers who use ATM machines to withdraw money, and the operator of a public open car park may want to use CCTV to monitor the safety of users and the security of vehicles parked;
- Collect relevant information to see whether CCTV will substantially solve the problem at hand. For example, if a property management company intends to use CCTV to tackle the problem of objects thrown from heights, records of similar incidents and the effectiveness of the use of CCTV to successfully prevent or detect the incident would be relevant;
- Assess whether there is genuine need for the use of high definition equipment to record detailed facial images of individuals. For example, detailed facial images are generally not required when CCTV is used for monitoring traffic flow or crowd movement;

[4] See www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/DH_e.pdf

- Any facial recognition system used in conjunction with CCTV must be supported by strong justification as the use of CCTV to enable automatic identification and tracking of individuals captured on CCTV footage is not normally expected by the public;

- Consult, where practicable, people who may be affected by the CCTV on what their concerns are, what steps may be taken to address these concerns and minimise the privacy intrusion;

- Covert CCTV surveillance should not be used without strong/overriding justification, and only as the last resort; and

- Clearly determine the scope or extent of monitoring. For example, it is not appropriate to use CCTV as a permanent measure when it was 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 installed in places where people have a reason to expect privacy (e.g. changing room). CCTV systems as a whole should be properly protected from vandalism or unlawful access.

People should be explicitly informed that they are subject to CCTV surveillance. An effective way is to put up conspicuous notices at the entrance to the monitored area and affix further notices inside the area as reinforcement. This is particularly important where the CCTV cameras themselves are very discreetly located, or located in places where people may not expect to be subject to surveillance (for example, in a taxi or a public light bus).

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

Proper Handling of the Recorded Images

DPP2(1) and **DPP2(2)** impose 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 securely deleted regularly if no incident of security concern is discovered or reported.

If third party contractors are engaged in the provision and/or maintenance of CCTV, and have access to the CCTV images containing personal data, **DPP2(3)** requires that data users must adopt contractual or other means to ensure that personal data accessible by contractors is not kept longer than necessary. Depending on the particular situation, data users may need to work with their contractors to ensure that this principle is complied with. For example, contractors engaged to extract footage from the CCTV system to fulfil data access requests received by data users must be instructed not to keep the footage longer than necessary. Data users may refer to the Information Leaflet "Outsourcing the Processing of Personal Data to Data Processor"[5] published by the Commissioner for details.

DPP4(1) requires data users to take all reasonably practicable steps to ensure that the personal data held by them is protected against unauthorised or accidental access, processing, erasure, loss or use.

[5] See www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf

Security measures must be in place to prevent unauthorised access to the CCTV system including proper access control defining who can access the recorded images and under what circumstances.

Recorded images, whether stored locally in the CCTV or remotely in a computer, should be kept in safe custody. There must also be sufficient safeguards in place to protect the wireless transmission systems for images, if used, from interception. Access to places where the images recorded by the CCTV cameras are viewed, stored or handled should be secured and restricted to authorised persons only. Proper logs of which staff members in custody of the recorded images should be updated on time. Transfers and movements of the recorded images should also be clearly documented.

Once there is no valid reason to retain the recorded images, they should be securely deleted.

If a data user engages contractors that would have access to the recorded images, **DPP4(2)** requires that the data user must adopt contractual or other means to ensure that there is no diminution in protection for the personal data accessible by contractors[6].

Transfer of CCTV Records to Third Parties

On the use of personal data, **DPP3** stipulates that personal data shall only be used for the purposes for which it was collected or a directly related purpose. Unless the data subject gives prescribed consent (which means express consent given voluntarily) or if any applicable exemptions under the Ordinance apply, personal data should not be used for a new purpose.

When a data user (e.g. building management company) is asked to provide copies of CCTV records to a law enforcement agency (e.g. the police) for criminal investigation purpose, the exemption provided under section 58(2) of the Ordinance[7] may apply. The data user, however, is under no general obligation to supply the personal data as requested. Before the exemption is invoked, the data user must be reasonably satisfied that failure to supply the data would likely prejudice the investigation.

Transparency of Policy and Practice

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

To meet this requirement, data users 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 is to be used and the retention policies are clearly set out and communicated internally and to the data subjects.

It is also important for data users to establish who has the responsibility to operate the CCTV system and control the zoom-in functions (if any), and to decide what is to be recorded, how the recorded images should be used, how the recording media is to be disposed of after use and to whom the recorded images may be disclosed.

The above policies or procedures should be 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 and 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 staff member so that appropriate follow up actions, including disciplinary actions, can be taken.

---

[6] See footnote 5

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

Regular Reviews

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

The justifications for the continued use of CCTV systems should be reviewed regularly to ensure that they are serving the purpose for which they were first installed. If such reviews indicate that the use of the CCTV is no longer relevant or necessary, or if less privacy intrusive alternatives can be used to achieve the same purpose, the data user should cease using the CCTV.

DRONES

There is no universally accepted definition for drones but typically they cover aircrafts that are either controlled autonomously by computers or by remote pilots.

Drones can be used in many ways that bring about great social and economic benefits, such as land surveying, predicting weather patterns, fighting fires, as well as search and rescue operations. They are also increasingly used in commercial operations (such as shooting advertisement, TV and movie production); and for hobby or recreational purposes.

The use of certain types of drones may be subject to regulation (including the need for a permit) by the Civil Aviation Department[8] and, if the remote control equipment is modified to extend its control range, the Office of the Communications Authority[9] in Hong Kong.

Privacy Intrusiveness of Drones

Drones can perform as powerful surveillance tools when fitted with cameras. The threats they pose to privacy are consistent with the use of CCTV. Hence the above guidelines for CCTV apply equally to the use of drones fitted with cameras.

Furthermore, drones can be far more privacy intrusive than CCTV in view of their unique attributes:

- Being small, portable, mobile and cheap, they can track an individual's activities more persistently over time and in places that are not expected while covering a wider area;
- They are a relatively covert form of surveillance as they are mobile and in practical terms, it is difficult for the public to know who the operators are; and
- When equipped with a full range of advanced surveillance technologies such as telephoto lens and infrared sensors, they would acquire sophisticated abilities such as capturing data from distances and through objects, and with a fine level of detail.

To eliminate or reduce the harmful effects of these highly privacy intrusive features, users of drones should be particularly mindful of the need to respect people's privacy. Public perception and the reasonable privacy expectations of affected individuals should be ascertained. The alternative use of less privacy intrusive means of collection and use of personal data should be seriously considered. The intrusion on privacy can only be justified if it is proportional to the benefit to be derived, or else it could amount to unfair collection of personal data under **DPP1(2)**.

Suggestions on Responsible Use

Some tips on the responsible use of drones are as follows:-

Flight path – Flight paths should be carefully planned so as to avoid flying close to other people or their properties. For example, drones should be launched from a location as close as possible to the area they need to cover.

[8] See www.cad.gov.hk/english/Unmanned_Aircraft_Systems.html
[9] See www.ofca.gov.hk

Recording and retention – If recording is intended, the recording criteria (what, where and when to record) should be pre-defined to avoid over-collection of information, some of which may be related to individuals. Drones may go off course by accident and record scenes unintentionally. A policy to erase irrelevant recording and a data retention policy should be developed.

Security – If images are transmitted through wireless means, encryption should be considered to avoid the adverse consequences of interception by unrelated parties. If the drone has a recording function, access control should be considered to prevent the recording from falling into the wrong hands in the event the drones are accidentally lost.

Notice – Being transparent about the operation of the drone is important to building trust with those affected by its operations. Informing them clearly of your purposes and operation details is the best first step to assure them that you have nothing to hide and are not covertly monitoring anyone. However, this often poses the greatest challenge and innovative approaches may be called for, such as:-

- flashing lights may be used to indicate that recording is taking;
- pre-announcing drone operations in the affected area by social media;
- putting corporate logo and contact details on drones;
- having crew members wear clothes with the same corporate identities; and
- putting up big banners with privacy notices and contact details at "launch sites".

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