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

07/10