LCQ15: Privacy issues involved in use of CCTV systems with automated facial recognition function

Following is a question by the Hon Charles Mok and a written reply by the Secretary for Constitutional and Mainland Affairs, Mr Patrick Nip, in the Legislative Council today (June 5):

Question:

At present, quite a number of government departments have installed closed-circuit television (CCTV) cameras at areas under their purview or public places for security and monitoring purposes. With the advancement in technology, the governments and commercial organisations in some other regions make use of high resolution CCTV systems with recording and automated facial recognition (AFR) functions (AFR-CCTV systems) to get to know the identity of persons in a footage by making comparisons between the footage and databases. Such a practice has given rise to controversies. In view of this, the governments of some overseas cities have recently banned the use of facial recognition technology by government departments (including law enforcement agencies), with a view to preventing the abusive use of such technology and excessive monitoring by government departments, thereby protecting the personal privacy of the public. In this connection, will the Government inform this Council:

(1) of the respective numbers of (a) CCTV cameras installed in government venues and public places by the various government departments (including the Hong Kong Police Force (HKPF) and other law enforcement agencies), and (b) body worn video cameras provided by such departments to their public officers, in each of the past three years, as well as (i) the uses of such devices and (ii) for how long they have been installed/provided (set out in a table);

(2) whether the various government departments (including HKPF and other law enforcement agencies) procured or developed AFR-CCTV systems or conducted trials of applying AFR technology in CCTV systems, in each of the past three years; if so, of the details and justifications for that;

(3) whether it will, in order to protect the public's privacy, ban government departments (including HKPF and other law enforcement agencies) from using systems and devices with AFR function in public places for collection of personal identifiable information and automatic comparison with databases; if so, of the details; if not, the reasons for that; and

(4) whether it will enact legislation to regulate the use of AFR-CCTV systems by commercial organisations, so as to prevent excessive collection of sensitive personal data; if so, of the details; if not, the reasons for that?

Reply:

President:

After consulting the relevant bureaux and the Office of the Privacy Commissioner for Personal Data, our consolidated reply is as follows:

(1) and (2) At present, a number of government departments have installed closed-circuit television (CCTV) cameras in areas under their purview or in public places, such as transport infrastructure and public rental housing estates, for various purposes such as daily security, anti-theft, protection of public safety and crowd management, etc. These departments mainly include:

The Hong Kong Police Force (HKPF) has installed around 250 CCTV systems along the land boundary and Hong Kong waters for purposes such as boundary security, anti-illegal immigration and anti-smuggling. The HKPF has also set up temporary CCTV cameras at strategic locations (including places where large crowds may appear) to assess pedestrian flow and movement during festivals and large-scale public events, so as to implement corresponding crowd management measures. Such temporary systems are not equipped with recording function and will be removed after the events. The Immigration Department and the Customs and Excise Department have installed 2,331 and 3,070 CCTV systems at control points respectively, to monitor crowd and vehicle movements at immigration control points and the operation of e-Channels as well as for general security purpose. The Housing Department has installed around 24,000 CCTV cameras at venues such as public rental housing estates and shopping arcades for security and anti-theft purposes. To monitor real-time traffic conditions, the Transport Department has set up around 770 CCTV systems on roads with busy traffic and within control areas. Operators at Area Traffic Control Centres may, through the CCTV data and having regard to real time traffic conditions, implement traffic management schemes. The Leisure and Cultural Services Department has set up 8,650 CCTV systems at its venues for maintaining public safety, assisting in crowd control and monitoring operation of the venues.

The above government departments deploying CCTV systems all have internal guidelines which state that only authorised officers are allowed to use the systems. The guidelines also ensure that the use of CCTV systems, the collection of recorded images and the handling of data comply with the Personal Data (Privacy) Ordinance (Cap 486) (PDPO).

With respect to body worn video cameras provided by government departments to public officers, the HKPF has issued over 2,200 body worn video cameras to their officers since 2013, and the Correctional Services Department has issued around 700 body worn video cameras to their officers since 2016, mainly for use in investigation, evidence-gathering, prosecution or complaint-handling. According to information provided by government departments, no government department has procured or developed AFR-CCTV systems or applied AFR technology in CCTV systems.

(3) and (4) Biometric data (such as facial features) is data directly related

to an individual. When the biometric data is linked with personal data in another database, or after data consolidation and analysis, a particular individual can be directly or indirectly identified. Therefore, biometric data (such as data of facial features captured by facial recognition technology) is also regarded as personal data under the PDPO and regulated by the provisions of the Ordinance.

The PDPO is applicable to both the public and private sectors. All public and private organisations, including government departments, are required to comply with the PDPO and its Data Protection Principles (DPPs) when collecting and using personal data. Before collecting biometric data, the public or private organisation must ensure there is a specific purpose and an actual need for it. Some exemptions for personal data held for the purposes of the prevention or detection of crime are provided for under section 58 of the PDPO. In general, DPP4(1) stipulates that a data user must take all practicable steps to ensure that any personal data held by him/her is protected against unauthorised or accidental access, processing, erasure, loss or use, having regard to the kind of data and the harm that could result from improper handling (as well as other factors).

To assist data users in complying with the requirements of the PDPO with respect to the collection of biometric data, the Privacy Commissioner for Personal Data published the Guidance on Collection and Use of Biometric Data. It provides a number of measures and recommendations to minimise the risk with regard to biometric data collection, which include:

- Data users who intend to collect biometric data must first consider whether the collection is necessary;
- Data subjects should be provided with a free and informed choice to allow the collection of their biometric data, together with a detailed explanation about the impact of the collection of such data on personal data privacy;
- Strict controls on the access to, use and transfer of biometric data should be imposed. An individual's biometric data should not be used for any purposes other than the ones for which it was originally collected (including disclosure to a third party) unless explicit and voluntary consent has been obtained in advance;
- For biometric data which is no longer required for the purpose for which it is collected, regular and frequent purge should be carried out;
- Measures should be taken to guard against any risk of compromising and thieving of the biometric database and ensure that effective security measures are implemented as are reasonably practicable in the particular circumstances. For example, the biometric data should be encrypted while it is being stored or transmitted;
- Regular privacy compliance assessments and reviews should be conducted to ensure that the acts done and practices engaged are in compliance with the Ordinance. Proper training, guidance and supervision have to be given to the staff responsible for the collection and management of the biometric data; and
- If contractors are engaged in the handling of personal data, contractual

or other means must be adopted to prevent personal data transferred to the contractor from being kept longer than necessary and from unauthorised or accidental access, processing, erasure, loss or use.