LCQ11: Facial and visual image recognition technologies

Following is a question by the Hon Charles Mok and a written reply by the Acting Secretary for Constitutional and Mainland Affairs, Mr Andy Chan, in the Legislative Council today (November 6):

Question:

Facial and visual image recognition technologies enable the identification of individuals' identity and vehicles' registration marks (number plates) by comparing videos or visual images with a database. It has been reported that earlier on, some police officers, when conducting searches on the belongings of passengers on board a public bus, used high-definition digital video cameras to record the faces of passengers at a close distance. Regarding the use of facial and visual image recognition technologies by various government departments and public organisations, will the Government inform this Council:

(1) whether the Hong Kong Police Force (HKPF) currently uses facial recognition technologies to conduct real-time facial recognition or visual image analyses; if so, when the use began, and set out in a table the following details by name of the systems:
(i) the supplier's name and place of registration,
(ii) the technologies and functions involved,
(iii) the procurement details (including the price and quantity), and
(iv) HKPF's departments which have installed the system and the details of the use, including (a) the commissioning date, (b) the lowest rank of the police officers who are allowed to operate the system, (c) the specific uses, and (d) whether the supplier can store and retrieve the data, the ownership of the data, as well as the policy and the authorisation arrangement for officers in respect of the storage, retrieval and use, retention and deletion of the data (data policy);

(2) whether HKPF has plans to procure the aforesaid recognition systems in the coming three years; if so, set out in a table the following details by type of the systems:
(i) the supplier's name and place of registration,
(ii) the technologies and functions involved,
(iii) the procurement details (including the estimated price and quantity), and
(iv) HKPF's departments which will install the systems and the plans for using such systems, including (a) the lowest rank of the police officers who will be allowed to operate the systems, (b) the projected commissioning date, (c) the specific uses and (d) the data policy;

(3) whether HKPF has requested the Transport Department (TD) to provide the videos or visual images that TD recorded at public places; if so, of the

relevant procedure;

(4) of the following details of the automatic number plate recognition systems currently used by (A) HKPF and (B) TD (if applicable), and set out the information in a table by department and name of the system:
(i) the supplier’s name and place of registration,
(ii) the technologies and functions involved,
(iii) the procurement details (including the price and quantity),
(iv) the commissioning date,
(v) the districts in which the system has been used and the number of such system,
(vi) the lowest rank of the officers who are allowed to operate the system, and
(vii) the data policy;

(5) whether it knows the following details of the facial recognition systems used by the Airport Authority Hong Kong (AAHK) in the Hong Kong International Airport (A) for the self-service e-security gates and (B) for other airport facilities (if applicable), and set out the information in a table by the facility installed with such system and by name of the system:
(i) the supplier's name and place of registration,
(ii) the technologies and functions involved,
(iii) the procurement details (including the price and quantity), and
(iv) the details of use, including (a) the commissioning date, (b) the person-times using the system last year, (c) the number and percentage of visitors who opted out on collection of their personal data last year, and (d) the data policy;

(6) of the following details regarding the use of facial recognition technologies by the Immigration Department (ImmD), and set out in a table the information by name of the system:
(i) the supplier's name and place of registration,
(ii) the technologies and functions involved,
(iii) the procurement details (including the price and quantity),
(iv) the names of the immigration control points installed with the system and the number of such system installed, as well as the details of use, including (a) the commissioning date, (b) the specific uses and (c) the data policy, and
(v) the lowest rank of the officers who are allowed to operate the system;

(7) whether HKPF has requested ImmD, other government departments and AAHK to provide, or obtained by way of shared databases from such departments/AAHK, the facial features data of members of the public to assist HKPF in its law enforcement; if so, whether HKPF has conducted facial recognition on such data to identify the identity of individuals (if so, of the details);

(8) whether HKPF has sought from or provided to (including by way of shared database) the Mainland authorities (including law enforcement agencies) the facial features data of Hong Kong people for law enforcement; if so, among the data requested or provided, whether there have been data used by HKPF/the Mainland authorities for identifying the identity of individuals; if so, of

the details;

(9) whether it has assessed if currently government departments and public organisations have, prior to their making video records in public spaces and their using the visual images so collected for facial recognition and visual image analyses, sufficient justifications to support the necessity and the legality of such actions;

(10) given that the public have not been fully consulted on matters relating to the use, by government departments and public organisations, of technologies such as facial recognition and visual image analysis, and that some members of the public are concerned about the privacy protection issues involved in the application of such technologies, whether the Government and public organisations will suspend the use of such technologies; and

(11) whether the Government, when making amendments to the Personal Data (Privacy) Ordinance (Cap. 486), will (i) include the definition for "sensitive personal data", (ii) formulate a code of practice to be followed by those government departments and public organisations which have decided to use facial recognition and image analysis technologies, and (iii) stipulate that those government departments and public organisations using such technologies should regularly make reports to a dedicated independent monitoring authority so as to ensure that a balance is struck between safeguarding public safety and facilitating criminal investigations and protecting human rights and privacy?

Reply:

President:

Based on the information provided by relevant bureaux including the Security Bureau, the Transport and Housing Bureau, the Information and Technology Bureau and the Office of the Privacy Commissioner for Personal Data (PCPD), our consolidated reply is as follows:

(1) to (3) and (6) to (8) The Police has always been proactively applying any technology that can assist law enforcement and investigation, and has from time to time reviewed the effectiveness of various types of investigation tools and equipment, including various computer software which are useful for the Police in identifying suspects in criminal investigations. The further information requested in the question is not appropriate for disclosure lest it should compromise the Police's technologies and capabilities in prevention and detection of crime.

One of the statutory duties of the Police is crime prevention and detection. Should there be a need to obtain any data from other departments or overseas law enforcement agencies in the course of criminal investigations, the Police will apply to do so through established procedures if it is legally feasible. The entire process will be in strict compliance with the relevant provisions of the Personal Data (Privacy) Ordinance (PDPO) and personal privacy will be respected in the use of data for investigation.

Personal data collected by the Police in the course of crime prevention and detection will not be excessive, and the data obtained will only be used for the purposes of crime detection and prevention. The means of data collection must be in full compliance with the law. The personal data will be retained having regard to the purpose of data collection and the required period of data retention. Once it is no longer necessary to use the personal data for the particular purpose, the data will be destroyed within a reasonable time unless further retention is otherwise required by law.

The Immigration Department (ImmD) has employed facial recognition technology in its Immigration Control System, the Next Generation Smart Identity Card System and the Next Generation Electronic Passport System. The technology is mainly used to verify the identities of cross-boundary passengers (including visitors and cross-boundary drivers who choose to use the vehicular e-Channel service), applicants of the Hong Kong Identity Card and applicants of the Hong Kong Special Administrative Region passport. Details are set out in Annex 1. In accessing the relevant data, ImmD, as the data user, always abides by the strict guidelines which regulate the data access procedures. The data access procedures can only be conducted by ImmD’s authorised personnel in accordance with the requirements for personal data protection under the PDPO and other relevant ordinances and regulations. Passengers/applicants' personal data would not be accessed or processed by any system contractors.

(4) and (5) The Hong Kong Police Force's Automatic Number Plate Recognition (ANPR) System is used by traffic enforcement officers for detecting vehicles involving four types of traffic contraventions, namely unlicensed vehicles, vehicles licensed to disqualified drivers, vehicles licensed to persons wanted for an outstanding traffic warrant and stolen vehicles. If a vehicle is suspected to be in connection with those four types of traffic contraventions, a police officer will stop the vehicle for further enquiry. The data collected by the system will not be used for purposes other than detection of those four types of traffic contraventions. Details of the system are set out in Annex 2.

Currently, ANPR technology is applied in the Transport Department's Speed Map Panel System, Access Control System at government public car parks, Toll Collection System in government tunnels and control areas as well as Toll Collection System for entry to Ma Wan. Details are set out in Annex 3.

The Airport Authority Hong Kong (AAHK) applies facial recognition technology only at e-Security Gates at the Hong Kong International Airport. The said technology is supplied by a Hong Kong-registered company called NEC HK Limited. Featuring the NEC's patent facial recognition technology (NeoFace), the e-Security Gates facilitate the checking of travel documents and ensure that the identities of passengers entering the airport restricted area match the information shown on their boarding passes. There are at present a total of 68 e-Security Gates at Terminal 1. Since the launch of service on August 29, 2018, the e-Security Gates have recorded a usage of more than 17.3 million passenger times, of which about 30 000, representing

about 0.17 per cent, opted out of facial recognition. The procurement cost of the facility is fully borne by the AAHK, and no government expenditure is involved.

The AAHK attaches great importance to protecting customers' privacy and personal data. In this regard, the AAHK has developed its Privacy Policy Statement and Personal Information Collection Statement to inform e-Security Gate users about how the AAHK collects, uses and safeguards the personal data. For details, please refer to the following link to the Privacy Policy Statement and Personal Information Collection Statement: www.hongkongairport.com/en/passenger-guide/airport-security/e-security-gates-privacy-policy.page

(9), (10) and (11) From the perspective of safeguarding personal data privacy, government departments and public organisations will make reference to internal guidelines when capturing images or videos and using CCTV systems in public spaces. These guidelines state that only authorised officers are allowed to use the systems, and seek to ensure that the use of the systems, the collection of recorded images and the handling of data are in compliance with the PDPO.

Currently, the PDPO regulates the protection of personal data. According to the Data Protection Principle (DPP) 1 under Schedule 1 of the PDPO, the collection of personal data has to be necessary or directly related to the purpose for which the data is collected, and the data collected should be necessary and adequate but not excessive for such purpose. DPP 4 also states that data users should take all practicable steps to ensure the personal data they hold are protected against unauthorised or accidental access, processing, erasure, loss or use, having particular regard to "the kind of the data and the harm that could result if any of those events take place". Therefore, data users should adopt stricter security measures for sensitive personal data. The PCPD is planning to issue guidelines on "sensitive personal data" and advise on best practice for collection, use, disclosure, transfer and protection of personal data which is more sensitive in nature.

In fact, biometric data (such as facial features captured by facial recognition technology) is data directly related to an individual. When 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 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 organisations / departments are required to comply with the PDPO and its relevant DPPs when collecting and using personal data. They should also ensure that the collection of biometric data is for specific purpose with genuine necessity before collecting the data.

The PCPD understands that the use and collection of biometric data would become more common. In this connection, it has published the Guidance on Collection and Use of Biometric Data to put forward a number of measures and recommendations for data users handling sensitive biometric data on

minimising the risk with regard to biometric data collection, and to assist organisations in collecting biometric data in a responsible manner. The guidelines 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, 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.