LCQ5: Access to communications information by law enforcement agencies

Following is a question by the Hon Charles Peter Mok and a reply by the Secretary for Security, Mr John Lee, in the Legislative Council today (January 8):

Question:

Article 30 of the Basic Law protects the enjoyment of freedom and privacy of communication by Hong Kong residents. Article 14 in Part II (The Hong Kong Bill of Rights) of the Hong Kong Bill of Rights Ordinance provides that no one shall be subjected to arbitrary or unlawful interference with his correspondence. The existing Interception of Communications and Surveillance Ordinance merely requires law enforcement agencies to seek authorisation from a panel judge before conducting postal interceptions and telecommunications interceptions, but it does not impose any regulation on the information (including communications content, metadata and personal data) in network communications (such as mobile phones and web servers). Moreover, a judgment handed down by the High Court on October 27, 2017 has pointed out that the Police must, unless in exigent circumstances, obtain a warrant from the Court before they may inspect the mobile phone of an arrestee. It has been reported that an arrestee recently indicated that some of the instant messaging records in his locked mobile phone had been admitted as part of the evidence by the prosecution, but he had never disclosed to the Police the password for unlocking his mobile phone since his arrest and he had not been informed before the court hearing of the Police having obtained a relevant warrant. In this connection, will the Government inform this Council:

(1) of the number of cases since June last year in which the Police seized and unlocked the mobile phones of arrestees and accessed the information therein and, among such cases, the number of those in which a warrant was obtained;

(2) since when the Police began to use hacking software or other cracking tool for unlocking mobile phones in order to access the instant messaging contents or other information therein; and

(3) whether the Government will (i) by drawing reference from the relevant legislation in Korea, Taiwan, Australia, the United Kingdom and the United States, introduce legislative amendments or enact legislation to regulate the work on the collection of electronic evidence by law enforcement agencies, and (ii) take the initiative to regularly publish details of the requests made by various law enforcement agencies to information and communication technology companies for disclosure of information, so as to enhance the transparency of law enforcement efforts and enable such transparency to reach

international standards?

Reply:

President,

Under the laws of Hong Kong, law enforcement agencies (LEAs) have the responsibility to prevent and detect crimes, so as to protect citizens' lives and properties. In the course of carrying out their responsibilities, LEAs may exercise the search and seizure powers conferred by relevant legislation, and seize and examine various objects of the suspected offence, including mobile phones and other similar devices.

According to the judgment on a case handed down by the High Court on October 27, 2017, Police officers may seize mobile phones found on an apprehended person or in or about the place at which they have been apprehended in accordance with section 50(6) of the Police Force Ordinance (Cap 232) (PFO), but may examine the content of these mobile phones without obtaining a warrant only in exigent circumstances. The judgment also points out that, in authorising a warrantless search of the digital content of mobile phones or other similar devices seized on arrest only in exigent circumstances, section 50(6) of PFO is constitutional and compliant with Article 14 of the Hong Kong Bill of Rights Ordinance (Cap 383) and Article 30 of the Basic Law. I understand that LEAs have all along adhered strictly to the principles as laid down in the judgment.

When conducting criminal investigations, if required, LEAs may apply to the Court in accordance with the relevant laws for a search warrant authorising the search of any premises and the seizure of objects, documents, and materials found in the premises. LEAs have to observe stringent requirements when applying for search warrants, swear an oath before the magistrate to confirm that there are reasons to suspect that items of value to an investigation are being kept in a search target, and set out clearly the justifications for as well as the scope of the search warrant being sought. LEAs also have to satisfactorily answer any questions raised by the magistrates, who may impose conditions when issuing a search warrant having regard to individual circumstances. If the magistrates do not consider the justification to be sufficient or applicable, they will refuse the issue of the search warrant.

Magistrates deal with applications for search warrants strictly in accordance with the law, having regard to the facts and particulars presented before them by LEA officers. We need to respect the authority, professionalism, independence, and credibility of the Court.

I must stress that applying to the Court for search warrants and applying for prescribed authorisations for covert operations under the Interception of Communications and Surveillance Ordinance (Cap 589) (ICSO) are two separate legal procedures for different purposes, and should not be mixed up. Search warrants are applied in accordance with the relevant legislation and have to be approved by the Court, the purpose of which are

for collecting evidence as documentary exhibits in Court. The information which operations under ICSO seek to collect is mainly used for intelligence. Both are stringent sets of procedures, and are strictly regulated and restricted by law.

As to the case mentioned by Hon Mok in the question, Police have already publicly clarified that it was conducted under magistrate-issued search warrant. Since the case has already entered legal proceedings, it is not appropriate for me to comment further on the case details.

My reply to various parts of the question raised by Hon Charles Mok is as follows:

(1) From June to November 2019, Police processed 1 429 cases that involved mobile phones as evidence. Among those cases, 3 721 mobile phones belonging to arrested persons or suspects were involved, and relevant cases were all processed with search warrants issued by the Court.

(2) Generally, Police would only conduct digital forensic examination on mobile phones after obtaining Court warrants. The examination and the evidence obtained would be adduced in the relevant open trials. As the critical technologies used for the examinations are confidential information, disclosing such information may reveal to criminals details of LEAs' operations, thus allowing criminals to take advantage by undermining LEAs' capabilities in combating serious crimes and maintaining public safety. As such, I cannot disclose the information.

I must stress that, regardless of the technology employed, and irrespective of whether the relevant operation was conducted under a search warrant issued by the Court or was conducted under ICSO, Police operations must be conducted legally strictly adhering to the relevant laws and regulations.

(3) The existing ICSO requires the disclosure of a host of prescribed information. The Commissioner on Interception of Communications and Surveillance (the Commissioner) is required by ICSO to provide an annual report setting out the information specified for disclosure. The reports are made public. They are tabled at the Legislative Council every year, and are discussed at the Panel on Security. The reports cover figures and types of operations, the results of the Commissioner's inspections, and whether there were cases of non-compliance and the relevant disciplinary actions, etc. This practice is similar to that in many overseas jurisdictions.

Requests for information relating to the detection of crime from network services providers are adequately regulated by laws, as LEAs must do so in compliance with the requirements of the Personal Data (Privacy) Ordinance (Cap 486) or under a search warrant. The Government considers the existing regime and practice suitable for the situation in Hong Kong and should continue to operate.

Thank you, President.