(Translation)

LC Paper No. CB(2)1391/14-15(01)

香港特別行政區政府
保安局

香港添馬添美道 2 號

The Government of the
Hong Kong Special Administrative Region
Security Bureau

2 Tim Mei Avenue, Tamar, Hong Kong

本函檔號 Our Ref.: SBCR 14/2/3231/94 Pt.18

來函檔號 Your Ref.:

電話號碼 TEL. NO.: 2810 2632
傳真號碼 FAX. NO.: 2877 0636

8 May 2015

Miss Betty MA
Legislative Council Secretariat
Legislative Council Complex
1 Legislative Council Road
Central, Hong Kong

Dear Miss MA,

Thank you for your letter dated 13 April 2015. Members of the Bills Committee on Interception of Communications and Surveillance (Amendment) Bill 2015 raised their views at the meetings on 9 April 2015 and 2 May 2015. Government's response to matters relating to the Bill is at Annex A.

Government's response to matters raised by Members which are beyond the scope of the Bill is at Annex B.

Yours sincerely,

(Millie NG)
for Secretary for Security

Encl (6 pages)

c.c.
Department of Justice
(Attn: Mr. Godfrey KAN, Senior Assistant Solicitor General
Ms Monica LAW, Senior Assistant Law Draftsman)

Provide expressly that the Commissioner may require any public officer or any other person to provide "any protected product" in his possession to the Commissioner, including any protected product that contains journalistic material

According to Clause 13 of the Bill, the amended section 53(1)(a) of the Interception of Communications and Surveillance Ordinance (the ICSO) (Cap. 589) would provide expressly that for the purpose of performing any of the Commissioner's functions, the Commissioner may require any public officer or any other person to provide the Commissioner "any protected product" in his possession or control to the Commissioner, including any protected product which contains any information that is or may be subject to legal professional privilege (LPP).

2. Hong Kong residents have the right to confidential legal advice under Article 35 of the Basic Law, and LPP is also protected at common law. To fully implement the former Commissioner's proposal concerning the checking of protected products, it is necessary to provide expressly in the ICSO that the Commissioner may obtain any protected product, including any protected product which contains information that is or may be subject to LPP for the purpose of a review or examination.

3. Under the ICSO, "journalistic material" (JM) means "any material acquired or created for the purposes of journalism". The nature of JM is different from that of information subject to LPP. Although Clause 13 does not refer to protected products containing JM, section 53(1)(a) as amended by Clause 13 would provide expressly that the Commissioner may obtain "any protected product". With the enactment of Clause 13, the Commissioner shall have the right, under section 53(1)(a) of the ICSO, to obtain and check any protected product which contains or may contain JM for the purpose of ascertaining whether the law enforcement agencies (LEAs) have complied with the relevant requirements.

Whether overseas supervisory bodies have express authority to check protected products

4. The Government has tried to approach supervisory bodies which oversee interception of communications and covert surveillance in other countries in writing, enquiring about the legislation, policies and arrangements for the checking of protected protects by such supervisory bodies.

5. Since interception of communications and covert surveillance is a highly sensitive subject to every country, the information that we can obtain from them is very limited. Based on the available information, we came to understand that the corresponding legislation of these countries did not confer an express authority on the supervisory bodies to check protected products. However, as indicated by some of these supervisory bodies, their legislation did not preclude them from doing so, and they all considered that they had the right to check protected products. As to whether they check protected products that are or may be subject to LPP, such these supervisory bodies did not provide any information.

Security Bureau
May 2015

Explain whether social media and instant messaging applications fall within the scope of the Interception of Communications and Surveillance Ordinance (ICSO) and the meaning of "intercepting act" and "communication transmitted by a telecommunications system"

Under section 8 of the ICSO, an officer of a law enforcement agency (LEA) may apply to a panel judge for the issue of a judge's authorization for any interception or Type 1 surveillance to be carried out by or on behalf of any of the officers of the LEA.

2. As defined in section 2(1) of the ICSO, "interception", in relation to any communication, means the carrying out of any intercepting act in respect of that communication; or when appearing in a context with no specific reference to any communication, means the carrying out of any intercepting act in respect of any communication; and "intercepting act", in relation to any communication, means the inspection of some or all of the contents of the communication, in the course of its transmission by a postal service or by a telecommunications system, by a person other than its sender or intended recipient.

3. Under the ICSO, if a communication is transmitted by a telecommunications system[1], and an LEA intercepts the communication in the course of its transmission, then the interception will be regarded as an "intercepting act". The LEA must obtain an authorization from a panel judge before it may conduct such interception, and such interception operations are subject to the oversight of the Commissioner on Interception of Communications and Surveillance (Commissioner).

4. The LEAs are required to act in accordance with the provisions of the ICSO, under which the intercepting act that requires authorization is clearly defined. Panel judges will carefully examine each and every application to ascertain if it fully complies with the requirements of the ICSO before making a determination.

5. Given that operations carried out by the LEAs under the ICSO are of a confidential nature, disclosing details of such operations may reveal their law enforcement capabilities to criminals, who may then be able to elude justice,

---

[1] The term "telecommunications system" in the ICSO has the same meaning as that given to the term section 2(1) of the Telecommunications Ordinance (Cap 106), i.e. "any telecommunications installation, or series of installations, for the carrying of communication by means of guided or unguided electromagnetic energy or both".

thus undermining the LEAs' ability to investigate crime and protect public security. Provision of further information is, therefore, inappropriate.

Requesting Subscribers' Information from Internet Service Providers

6. When investigating crime, LEAs may, depending on the nature of the cases and for the purpose of crime prevention and detection, request necessary information related to crime detection from the individuals or organisations concerned, including subscribers' information (such as account name and Internet Protocol address) and log records from local or overseas Internet service providers (ISPs), for locating witnesses, evidence or suspects. Such enquiries do not involve any request for records of the content of any non-public communications. LEAs are required to abide by the provisions of the Personal Data (Privacy) Ordinance (Cap. 486) when requesting personal data for the purpose of crime prevention and detection. Requesting subscribers' information from ISPs is part of LEAs' routine law enforcement efforts, and falls outside the scope of the ICSO.

7. Generally, LEAs will, for the purpose of combating technology crimes and offences committed through the Internet, request information relating to the case under investigation from ISPs when necessary. Types of such cases include dissemination of child pornography, naked chat blackmail, online business fraud, email or social media scams, distributed denial-of-service attacks, unauthorised access to a computer system, access to a computer with a criminal or dishonest intent, using or distributing infringing copies of copyright works or counterfeit goods, and offences relating to corrupt transactions.

LEAs' Application for Court Warrants

8. For the purpose of crime investigation, LEAs may apply to the court in accordance with relevant laws for a court warrant authorizing the search of any premises or place.

9. There are pieces of legislation in Hong Kong which provide for an application for a court warrant. Depending on the circumstances of individual cases, LEAs may apply for court warrants according to theselegislation and execute the same in accordance with the statutory requirements as well as any conditions imposed in the warrants. Legislation that provides for an application for a court warrant includes: section 17 of the Prevention of Bribery Ordinance (Cap. 201), section 10B of the Independent Commission Against Corruption Ordinance (Cap. 204), section 50(7) of the Police Force Ordinance (Cap. 232), section 5 of the Organized and Serious Crimes Ordinance (Cap. 455), section 191 of the Securities and Futures Ordinance (Cap. 571), section 21

of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405), section 123 of the Copyright Ordinance (Cap. 528) and section 56AA of the Immigration Ordinance (Cap. 115).

10. LEAs have to observe stringent requirements when applying for search warrants from magistrates. Apart from completing an "Information for Search Warrant" form and a "Search Warrant" form, LEAs are required to swear an oath before the magistrate to show that there are reasons to suspect that items of value to an investigation are being kept in a building or a place. In addition, LEAs have to clearly set out the justifications for applying for a search warrant as well as the scope of the search warrant being sought when making their application, which shall include the offences involved in the case, locations of the premises and so on, and, at the same time, answer any questions raised by the magistrates. Once issued, the search warrant shall be sealed by the Court and the relevant particulars will be put on record. LEAs will then have to act in strict compliance with the search warrant, including any conditions imposed by the magistrate.

11. Regarding the execution of a search warrant, LEAs generally have to produce the warrant to the occupier of the premises and, when necessary, a copy of the search warrant shall also be made available. Even if the operation concerned has yet to be turned overt, it shall become overt soon after the approval of the application. In this connection, execution of a search warrant is an operation conducted in an overt manner.

12. In any prosecution, the search warrant will generally be disclosed by the prosecution. If the defence considers that there is any impropriety in the issue of the warrant, they may apply to the court to have the evidence obtained under the warrant excluded from the trial, or, if the impropriety is serious enough, to have the proceedings permanently stayed.

13. The arrangements for LEAs applying for court warrants to obtain documents or information from ISPs are substantially the same as those for applying court warrants to obtain documents or information from other organisations and individuals. These operations are part of LEAs' routine law enforcement efforts and do not fall within the scope of the ICSO.

Intelligence Management

14. At present, information obtained as a result of a covert operation, together with the information obtained by an LEA from other sources such as

crime reports from the public, case investigation and open source materials, can be aggregated into intelligence after being screened, evaluated and analysed. The intelligence will be used by the LEA for the purpose of crime prevention or detection. The intelligence management system of an LEA is subject to tight control. An LEA must strictly comply with its internal guidelines to ensure that all steps including the input, storage, access, use, updating, disposal or destruction of intelligence are under stringent internal control and audit. Audit trail record is kept for all access to and processing of intelligence, thereby ensuring system security and accuracy and reliability of intelligence.

Security Bureau
May 2015