(Translation)

LC Paper No. CB(2)1732/14-15(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.19

來函檔號 Your Ref.:

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

19 June 2015

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

Dear Miss MA,

Members of the Bills Committee on Interception of Communications and Surveillance (Amendment) Bill 2015 enquired about the breakdowns of technology crimes (by nature of crimes) and statistical figures of law enforcement agencies' application for court warrants maintained by the Judiciary at the meeting on 1 June 2015. Government's response is at Annex A.

Government's response to written submissions from deputations at the Bills Committee's meeting on 2 May 2015 is at Annex B.

Yours sincerely,

(Mrs Millie Ng)
for Secretary for Security

Encl (15 pages)

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

ICS(A)2015-04
Annex A

Breakdowns of Technology Crimes (by nature of crimes)

Law enforcement agencies (LEAs) will, for the purpose of combating technology crimes and offences committed through the Internet, request information relating to the case under investigation from internet service providers (ISPs) when necessary. This is part of LEA's routine law enforcement efforts and does not fall within the scope of the Interception of Communications and Surveillance Ordinance (the ICSO) (Cap. 589). Breakdowns of technology crimes (by nature of crimes) recorded by the Police in 2013 and 2014 are as follows:

Technology Crime Figures Recorded by the Police in 2013 and 2014

Case nature	2013	2014
Online Game Related	425	426
Online Business Fraud (including e-auction, online shopping, online commercial fraud and credit card misuse)	1 449	2 375
Unauthorized Access to Computer (including Internet/email account abuse, hacking activities)	1 986	1 477
Others	1 273	2 500
Miscellaneous Fraud (including social media deception)	*435*	*1 436*
Child Pornography	*41*	*38*
Distributed Denial of Service (DDoS) Attacks	*3*	*29*
e-Banking	*40*	*17*
Naked Chat-related Blackmail	*477*	*638*
Others	*277*	*342*
Total	**5 133**	**6 778**

Statistical figures of LEAs' application for court warrants maintained by the Judiciary

2. 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. Applying for court warrants to obtain documents or information from any organizations and individuals is part of LEAs' routine law enforcement efforts and does not fall within the scope of the ICSO. LEAs have to observe stringent requirements when applying for search warrants from magistrates. Once a search warrant is issued, LEAs must act in accordance with the search warrant, including any conditions imposed by the magistrate.

3. The arrangements for LEAs applying for court warrants to obtain documents or information from ISPs are substantially the same as those for applying for court warrants to obtain documents or information from other organizations and individuals. According to Government's enquiries to the Judiciary, the courts do not maintain statistics on the number of LEAs' applications for court warrants, nor do they keep any relevant statistics on the number of approved and rejected LEAs' applications.

Security Bureau
June 2015

Government's response to written submissions from deputations at the Bills Committee's meeting on 2 May 2015

	Issues	Responses
1.	**Safeguards for journalistic material (JM)** (a) Safeguards for JM should align with those for information subject to legal professional privilege (LPP)	(a) In handling cases where JM is likely to be involved, the mechanism under the existing ICSO has provided sufficient safeguards on the premise of striking a balance between prevention and detection of serious crimes and protection of press freedom. It is stipulated in Schedule 3 to the ICSO that when applying for an authorization to conduct any covert operation, the LEA officer concerned has to set out in the affidavit or written statement supporting the application an assessment of the likelihood of obtaining information which may be the contents of JM. The panel judge concerned will consider whether or not a prescribed authorization should be issued, taking into account the applicant's assessment, and will impose additional conditions on all cases assessed to have a likelihood of obtaining JM for ensuring better protection of press freedom. Separately, paragraph 65 of the Code of Practice (COP) was revised in 2011 to require that all applications for prescribed authorization for Type 2 surveillance with the likelihood of obtaining JM should be considered by panel judges.

	Issues	Responses
		If JM has been obtained or will likely be obtained as assessed in the interception operation, the LEA concerned has to submit a report to the panel judge who will, based on the report, consider whether the conditions for the continuance of the prescribed authorization are still met in order to determine whether such an authorization should be revoked. Panel judges exercise caution in examining each and every case in which JM is involved, and they will impose restrictive conditions if necessary. The prescribed authorization will be revoked if the panel judge considers that it no longer meets the conditions stated in section 3 of the ICSO. As stated in paragraph 121 of the COP, the Commissioner should be notified of cases where information which may be the contents of any JM has been obtained or will likely be obtained by LEA officers through interception or covert surveillance operations. The LEA concerned has to preserve, in compliance with the Commissioner's request, the relevant interception products for his case review.
	(b) Empowering the Commissioner to listen to the contents of conversations intercepted by law enforcement officers is welcomed. When exercising his power to check protected products involving JM, the	(b) According to Clause 13 of the Bill, the amended section 53(1)(a) of the ICSO will 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 "any protected product" in his possession or control to the Commissioner. If the Bill is enacted into law, the Commissioner will have the right, under

	Issues	Responses
	Commissioner has to ensure that the checking of such contents is solely for the purpose of examining whether the conduct of the law enforcement officers is proper, and that the contents concerned should not be disclosed to irrelevant parties. Such safeguards should be stipulated in the provisions.	section 53(1)(a) of the ICSO, to request and check any protected product which contains or may contain JM for the purpose of ascertaining whether LEAs have complied with the relevant requirements. This proposed amendment will help enhance protection of press freedom.
2.	No restriction or regulation is in place under the ICSO on the acts carried out by overseas law enforcement officers or local non-public officers.	Between 1996 and 2006, the Law Reform Commission (LRC) published five reports on privacy, including the reports on *Regulating the Interception of Communications* and *The Regulation of Covert Surveillance*. Recommendations have been made in these reports on intentional interception of, or interference with, a communication in the course of its transmission, as well as trespass into private premises and the use of a surveillance device for covert surveillance. To implement the parts relating to public officers in the above two reports, the Government introduced the ICSO in 2006 to regulate the interception of communications and covert surveillance by the specified LEAs under a stringent statutory regime. The main purpose and scope of the ICSO is to regulate the specified LEAs' interception of communications and covert surveillance for prevention and detection of serious crimes and protection of public

	Issues	Responses
		security. The ICSO is not applicable to non-public officers nor to non-governmental bodies and individuals. According to the information provided by the bureaux concerned, any acts of interception of communications by non-public officers may constitute a contravention of section 24 of the Telecommunications Ordinance (wilful interception of messages by a telecommunications officer) or a contravention of section 27 of the same (damaging telecommunications installation with intent). Such acts are subject to the Personal Data (Privacy) Ordinance if they involve the collection of personal data. Upon the publication of the two LRC reports on *Regulating the Interception of Communications* and *The Regulation of Covert Surveillance*, the Hong Kong news media and journalists expressed concern that the recommendations might undermine press freedom. Since the five LRC reports on privacy touch on a sensitive and controversial policy and political issue, namely how to strike a balance between protection of individual privacy and freedom of the media, they are handled by stages. The bureau concerned first dealt with the report on *Stalking*, which was comparatively less controversial, by conducting public consultation, commissioning a consultancy study and presenting the topic for discussion at the Legislative Council Panel on Constitutional Affairs (CA Panel) on three occasions. None of the various formulations is supported by CA Panel Members, major stakeholders or the general public, as being able to achieve the objective of providing protection to all

	Issues	Responses
		people alike against stalking while at the same time avoid inflicting interference to the freedoms of the press and expression. In this connection, the bureau concerned is of the view that there are no favourable conditions to pursue the matter further, and they will continue to monitor related developments in considering the way forward.
3.	A person who carries out activities in a public place is entitled to a reasonable expectation of privacy. There are no provisions in the ICSO regulating LEA's conduct of covert surveillance on a person carrying out activities in a public place. A monitoring mechanism should be put in place to guard against any improper political surveillance by the Government in a public place.	According to section 2(1) of the ICSO, "covert surveillance" means any surveillance carried out with the use of any surveillance device in the specified circumstances for the purposes of a specific investigation or operation, including where the proposed surveillance is carried out in circumstances where any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy, as specified in paragraph (a)(i) of the definition of "covert surveillance". According to section 2(2) of the ICSO, for the purposes of the Ordinance, a person is not regarded as being entitled to a reasonable expectation of privacy within the meaning of paragraph (a)(i) of the definition of "covert surveillance" in subsection (1) in relation to any activity carried out by him in a public place, but this provision does not affect any such entitlement of the person in relation to words spoken, written or read by him in a public place. In response to the views of the Bills Committee during the scrutiny of the Interception of Communications and Surveillance Bill in 2006, the Government had amended clause 2(2) of that Bill, i.e "a person is not regarded as being entitled to a reasonable expectation of privacy within

	Issues	Responses
		the meaning of paragraph (a)(i) of the definition of 'covert surveillance' in subsection (1) in relation to any activity carried out by him in a public place", by adding immediately thereafter "*but nothing in this subsection affects any such entitlement of the person in relation to words spoken, written or read by him in a public place.*" Activities carried out in a public place would be visible to any members of the public, and the person involved should have no reasonable expectation that such "activities" are not being observed by others. No authorization is therefore required for the conduct of surveillance operations in a public place for law enforcement purposes. However, this does not affect any reasonable expectation of privacy that the person may have in relation to words spoken, written or read by him in a public place. In other words, a person having a conversation in a public place may be entitled to a reasonable expectation of privacy in relation to the content of his conversation, while a person writing a letter in a public place may be entitled to a reasonable expectation of privacy in relation to the content of his letter. The Government considers that the statutory requirements for covert surveillance regarding the reasonable expectation of privacy that a person is entitled to enjoy in a public place have struck an appropriate balance between prevention and detection of serious crimes and protection of public security on the one hand, and protection of privacy as well as other individual rights on the other.

	Issues	Responses
4.	As far as the examination mechanism is concerned, the notification given by the Commissioner or order for payment of compensation made by him should not be limited to persons applying for an examination or those affected by acts of non-compliance, but should cover all persons subjected to interception and covert surveillance.	Pursuant to section 43 of the ICSO, a person may apply in writing to the Commissioner for an examination if he suspects that he is the subject of any interception or covert surveillance carried out by officers of an LEA. Upon receiving such an application, the Commissioner shall, unless he refuses to carry out an examination on a ground mentioned in section 45(1), carry out an examination to determine: (a) whether or not the interception or covert surveillance alleged has taken place; and (b) if so, whether or not such interception or covert surveillance has been carried out by an officer of an LEA without the authority of a prescribed authorization.. After the examination, if the Commissioner finds the case in the applicant's favour, he shall notify the applicant and initiate the procedure for awarding payment of compensation to him by the Government. Section 48 requires the Commissioner to give notice to the relevant person whenever the Commissioner, in the course of performing the functions under the ICSO, finds that any interception or covert surveillance has been carried out by an officer of any one of the four LEAs covered by the ICSO without a prescribed authorization. However, section 44(6) and section 48(3) provide that the Commissioner shall only give a notice when he considers that doing so would not be prejudicial to the prevention or detection of crime or the protection of public security.

	Issues	Responses
		As seen from the above, the notification mechanism under the ICSO applies not only to a person who has applied to the Commissioner for an examination but also to relevant persons affected by any unauthorized operations which come to the notice of the Commissioner in the performance of his functions. The ICSO does not empower the Commissioner to give notice to subjects affected by *lawful* interception or covert surveillance. It is inevitable that interception of communications and covert surveillance are conducted in a clandestine manner, and therefore the purpose of such operations is in conflict with any arrangement of giving notice to the subjects. Providing comprehensive notification would affect the efficacy of LEAs' operations. The threats targeted by the interception or surveillance might persist for a long period of time after the operation has ceased. In this connection, notifying the affected persons subsequent to the operations might also reveal the modus operandi and fields of operation of LEAs and their officers, which may compromise the effectiveness of law enforcement and may even endanger the safety of the officers, victims and witnesses. Criminals may also circumvent the law as a consequence. Restrictive measures in relation to the notification mechanism under the ICSO have struck an appropriate balance between maintaining the effectiveness of law enforcement and protecting the privacy of individuals.

	Issues	Responses
5.	The Government should conduct a review and create a criminal offence of unauthorized interception of communications or covert surveillance. Criminal liability should be imposed by the ICSO to punish such unauthorized interception or surveillance.	The LEAs will deal with any contravention of the requirements under the ICSO by their officers in accordance with their disciplinary mechanism, and the results of any disciplinary actions taken will be published in the Commissioner's Annual Report. The COP specifies that LEAs should take into account any views that the Commissioner may have on the appropriate disciplinary action before taking any disciplinary action against the offending officer. LEAs have been acting in accordance with this requirement. Besides, any public officer who has intentionally conducted interception of communications or covert surveillance without an authorization may constitute the common law offence of "misconduct in public office" and may be liable to imprisonment in serious cases. Regarding the need for imposing penalties for unauthorized interception of communications or covert surveillance, we consider that the matter should be dealt with in a holistic manner and that public officers and non-public officers should be treated on an equal footing. At present, the Government does not have plans to impose criminal liability under the ICSO for unauthorized acts committed by public officers.
6.	A more specific explanation on the definitions of "public security" and "violent means" should be given in the ICSO.	It is stipulated in the ICSO that the LEAs may conduct interception of communications and covert surveillance for the purpose of "protecting public security". Section 2(1) of the ICSO provides that "public security" means the public

	Issues	Responses
	The ICSO should be amended to prohibit all kinds of political surveillance and interception.	security of Hong Kong. Schedule 3 also requires that, if an application for a prescribed authorization involves "public security", the LEA should provide an assessment of the particular threat to public security, an assessment of its immediacy and gravity, and an assessment of its impact, both direct and indirect, on the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong in the affidavit or statement supporting the application. Section 2(7) of the ICSO also clearly provides that for the purposes of the Ordinance, advocacy, protest or dissent (whether in furtherance of a political or social objective or otherwise), unless likely to be carried on by violent means, is not of itself regarded as a threat to public security. Paragraph 37 of the COP also states: "The determination of what constitutes a threat to Hong Kong's public security is highly fact-based. Possible examples of such threats include activities connected with the illicit trafficking of weapons of mass destruction, terrorism-related activities, human trafficking, etc. Schedule 3 of the ICSO requires an assessment of the impact, both direct and indirect, of the particular threat to the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong for applications made on grounds of public security. … Advocacy, protest or dissent (whether in furtherance of a political or social objective or otherwise), unless likely to be carried on by violent means, is ***not*** of itself regarded as a threat to public security. Grounds for believing that violent means are likely must be included in

	Issues	Responses
		the application involving such activities. "Violence" does not cover minor scuffles or minor vandalism etc. Furthermore, any applications for authorization must comply with the following statement made by the Secretary for Security during the Second Reading Debate of the Interception of Communications and Surveillance Bill on 2 August 2006: '*Law enforcement agencies will under no circumstances undertake surveillance operations under the Bill on grounds of public security to achieve a political objective. … The powers under the Bill after its passage will not be used for investigation of criminal offences that are yet to be created under Article 23 of the Basic Law.* '" As seen from the above, the LEAs are bound by the requirements of the ICSO and COP. Under no circumstances may they conduct covert operations regulated by the ICSO for achieving a political objective on grounds of public security. All applications for authorization made by LEAs must comply with the stringent conditions under the ICSO. Apart from the requirement that the purpose of an operation must be for the prevention or detection of serious crimes or the protection of public security, the proposed operation must also be able to meet the "proportionality" and "necessity" tests before the panel judge or authorizing officer would grant their approval. LEA's operations under the ICSO would also be subject to stringent oversight of the Commissioner. The Government has no intention to revise the definition of "public security" under the existing ICSO.

	Issues	Responses
7.	Supervision of the storage of surveillance devices should be enhanced; specific supervisory provisions should be laid down on the handling of removable storage media (e.g. memory cards, discs and tapes) in surveillance devices.	The Commissioner has all along required the LEAs to develop a comprehensive system for the recording of surveillance devices, as a means to monitor and control the devices, as well as to restrict their use only for authorized and lawful purposes. At present, the LEAs have established a control mechanism for the issuance and receipt of surveillance devices. The issuance and receipt of all surveillance devices have to be properly documented in the device registers. Copies of both the up-to-date inventory list and device registers are provided to the Commissioner regularly. Where necessary, LEAs are also required to provide copies of the device request forms for his examination. In case of discrepancies or doubts identified as a result of checking the contents of these copies and comparing with the information provided in the weekly report forms and other relevant documents, the Commissioner would require the LEA concerned to provide clarification and explanation. The Commissioner would also make inspection visits to the LEAs' device stores. In the case of an incident involving a surveillance device, the LEA is required to report to the Commissioner. As regards the handling of removable storage media, the Commissioner recommended in his 2012 Annual Report that the removable storage media (e.g. memory cards, discs and tapes) for surveillance devices should be handled by the LEAs in a secure and strictly regulated manner akin to the withdrawal and return of surveillance devices so as to avoid any possibility of these storage media being substituted, or in any way

	Issues	Responses
		tampered with. The Commissioner also recommended that a serial number should be assigned to each of the removable storage media and a computerized Device Management System should be used to control the issuance and receipt of storage media. Measures are being taken by the LEAs to take forward the arrangements in response to the Commissioner's recommendations.
8.	The definition of "communication" under the ICSO should be expanded by including "internet communication" in the scope of "communication". Clarification is sought on the regulation of LEAs' requests for metadata from ISPs.	Detailed responses of the Government are at Annex B of Paper No. ICS(A)2015-02 (LC Paper No. CB(2)1391/14-15(01)) issued to the LegCo Secretariat on 8 May 2015. The Government considers that the definition under the ICSO has been effective and has no plan to make amendments.

Security Bureau
June 2015