For information

17 May 2006 **SB Ref: ICSB 9/06**

Bills Committee on Interception of Communications and Surveillance Bill

Response to issues raised at the Bills Committee Meeting held on 9 May 2006

This note sets out the Administration's response to the points raised at the meeting of the Bills Committee on 9 May 2006 on the long title and certain definitions in clause 2(1) of the Bill.

Long Title

Issue 1 : To consider spelling out in the long title that the Bill sought to protect the freedom and privacy of communication of Hong Kong residents as provided in Article 30 of the Basic Law (BL30).

2. The present Bill is not the only relevant legislation that may be relevant to BL30, particularly when it only seeks to regulate the conduct of public officers. Therefore, we consider that the present long title, by referring to the conduct being regulated, is an accurate reflection of the purpose of the Bill, and do not consider it necessary to include a reference to BL30. In any event, it is usually not necessary for our domestic legislation to include an express reference, either in its long title or in the detailed provisions, to specific articles of the Basic Law that the legislation seeks to implement.

Clause 2(1) : Definition of "Copy"

Issue 2 : To consider amending sub-clause (a)(i) under the definition of "copy" in clause 2(1) of the Bill along the lines of "any copy, extract or summary of material which in substance is a copy, extract or summary of the material or identifies itself as such copy, extract or summary of such contents".

3. As explained at the Bills Committee meeting on 9 May 2006, the present formulation, which defines "copy" as including any copy, extract or summary of the material / contents "which identifies itself as" such copy, extract or summary of the material / contents, is modeled on the relevant

provision of the United Kingdom (UK) Regulation of Investigatory Powers Act 2000 (section 15(8)). In view of the concerns of some Members over the drafting of the expression, we propose to adopt an alternative formulation as follows –

"*any copy, extract or summary of such contents;*"

If this formulation is agreed, then paragraph (b)(i) and (ii) of this definition (and similar reference in the like definition in clause 65(3)) will also be amended along the same line.

Clause 2(1) : Definition of "Covert Surveillance"

4. Members raised various issues on the definition of "covert surveillance". Similar questions were discussed at meetings of the Panel on Security. Before responding to the specific issues raised at the meeting on 9 May 2006, we enclose at **Annex** for Members' reference extracts of the relevant papers submitted to the Panel, and summarize the main points as follows –

(a) The statutory regulation of covert surveillance is a developing subject among common law jurisdictions. The **legislative regimes of comparable common law jurisdictions vary considerably** –

- The **United States** (US) statutory regimes cover the use of devices to monitor and record communications only. Operations require judicial or executive authorization.
- The **UK** statutory regime, enacted in 2000, is more up to date and comprehensive in terms of coverage of types of covert surveillance operations. However, all operations require only executive authorization.
- **Australia**'s legislation enacted in 2004 is the most recent, and covers types of covert surveillance operations as comprehensively as our Bill, i.e., operations using listening, data surveillance, optical surveillance, and tracking devices. More intrusive operations are approved judicially, and less intrusive operations are approved executively.

(b) The relevant legislation of these jurisdictions generally does **not regulate** those covert surveillance operations by LEAs such as **tailing**

or monitoring a target without a device.

(c) In respect of **"participant monitoring"**, even if they are done with devices, such operations do not require statutory authorization under the relevant US and Australian legislation. Our Bill imposes a stricter regime by requiring executive authorization for such operations, confining such operations to the purposes of preventing or detecting serious crime or protecting public security, and subjecting them to the full range of other safeguards under the proposed legislation, e.g., oversight by the Commissioner on Interception of Communications and Surveillance, measures to safeguard the products etc.

(d) In carrying out covert operations without using devices, our law enforcement agencies (LEAs) are **subject to the applicable statutory or common law**. For example, LEAs would be liable for trespass under common law if they enter private premises without consent. The Bill does not seek to change the position.

5. Turning to the specific questions raised by Members at the meeting on 9 May 2006, our response is as follows.

Issue 3 : To provide information on methods used by law enforcement agencies, the devices used and the types of surveillance that fall within the meaning of "covert surveillance".

6. Surveillance operations done covertly by LEAs include –

(a) the "covert surveillance" operations defined in our Bill, using devices referred to in the Bill; and

(b) operations mentioned in paragraph 4 above, i.e., monitoring a target without using devices, or participant monitoring without devices.

7. At the meeting of the Bills Committee on 9 May 2006, some Members asked if we could elaborate the term "systematic" in the definition of "covert surveillance". As explained by the Administration at the meeting, the term has been included to exclude situations requiring a spontaneous response. While we consider that the term is a precise reflection of the intention, in view of Members' concern, we have no objection to deleting the term from paragraph (a) of the definition of "covert surveillance" and expanding paragraph (b) along the following lines –

"does not include –

(i) any spontaneous reaction to unforeseen events or circumstances; and

(ii) any such surveillance to the extent that it constitutes interception under this Ordinance;"

Issue 4 : To reconsider whether the scope of "covert surveillance" should be confined to those cases in which surveillance device is used.

Issue 5 : To provide information on the law which governs covert surveillance by undercover agents without use of surveillance device.

Issue 6 : To explain why surveillance carried out by a participating party or undercover agent without the use of device is not covered under the Bill.

8. Law enforcement operations not using devices mean **operations using only the human senses**. The human eye and ear are limited in their ability to intrude into privacy, and we all have a reasonable understanding of what others' eyes and ears can do. We know, for example, that eyes cannot see through curtains, and ears cannot hear conversations beyond a distance. That enables one to protect one's privacy if one wants to.

9. If an activity being monitored is carried out in a place which is accessible to the public, the monitoring without using a device should not give rise to any privacy concern. Where there is reasonable expectation of privacy, such as two persons whispering to each other in a public place, it is not possible to keep the surveillance covert and not alerting the persons to the surveillance, without using a device. If an activity takes place in private premises, the LEAs would be liable for trespass under common law as well as for any unlawful act that they may carry out on the premises, if they enter premises without lawful authority. Our LEAs would not carry out unlawful activities.

10. As noted above, it is usual among common law jurisdictions to confine their relevant legislation to operations using devices. In Hong Kong, it is neither a tort nor an offence for a person to follow another person in a public place without the latter knowing it.

11. As for **"participant monitoring" (including undercover operations)**, such operations in the US and Australia do not require statutory authorization whether devices are used or not (while our Bill imposes a stricter regime by requiring executive authorization for such operations if they involve the use of devices and subjecting the operations to the full range of safeguards).

12. As for **case law** in these jurisdictions, "participant monitoring" is generally regarded to be less intrusive. For example –

(a) US : the US Supreme Court has ruled that undercover operations in which an LEA officer conceals his identity do not invade the target's constitutionally justifiable expectations of privacy under the Fourth Amendment to the US Constitution, irrespective of whether electronic devices are used[1]. The Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it"[2].

(b) Canada : Case law in Canada draws a distinction between making a permanent electronic recording on conversations and simply listening to someone's words and repeating them afterwards. The Canadian court considers that the risk that someone will listen to one's words with the intention of repeating them and the risk involved when someone listens to them while making a *permanent electronic record* of them are of a different order of magnitude. "The law recognizes that we inherently have to bear the risk of the 'tattletale'"[3].

(c) Australia : The High court of Australia has ruled that[4] "Subterfuge, ruses and tricks may be lawfully employed by the police, acting in the public interest …. The critical question is not whether the accused has been tricked and secretly recorded. It is not even whether the trick has resulted in self-incrimination, electronically preserved to do greater damage to the accused at trial."

(d) UK : Invasion of privacy is not yet a tort in England and Wales.

13. In Hong Kong, the court has also recognized undercover operations as an essential part of LEAs' investigation techniques[5].

14. Surveillance not using devices is also carried out by members of the public. Collection of data by openly listening to, or taking part in conversations, is used throughout our society for many legitimate purposes. Not all listeners disclose to others what they have heard. Where they do, however, the concern is more with confidentiality than privacy. Our LEAs only conduct

---

1 United States v White, 401 U.S. 745 (1971).
2 Hoffa v United States, 385 U.S. 302 (1966).
3 R v Duarte [1990] 1 SRC 30.
4 R v Swaffield and Pavic ([1998] High Court of Australia).
5 FACC No. 9 of 1999, Secretary for Justice v LAM Tat-ming and NG Sai-hung; HKSAR v HEUNG Yu-nam [1997] 3 HKC 632 at 639, CA.

surveillance without device for law enforcement purposes.

Security Bureau
May 2006

Annex

Interception of Communications and Surveillance Bill

Definition of "Covert Surveillance"

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 21 February 2006

Item 5 : To explain why the Administration considers that the use of devices involving a party participating in the relevant communications is less intrusive, and to consider the suggestion of vesting the authority to authorise "less intrusive" covert surveillance operations with magistrates.

13. There are a number of situations under which collection of information through a participating party may be involved. For example, that party may be an undercover officer investigating a crime, or a victim of crime assisting the LEAs to gather evidence, or someone in a criminal syndicate who has decided to assist the LEAs in prevention or detection of serious criminal offences. Any disclosure made by the target person to the participating party would be done in the full knowledge of the presence of the party, and the risk that the party may further disclose the information to another person. An individual may consider that he is disclosing the information in confidence, but confidentiality is different from privacy. In its 1996 report on interception of communications, the LRC discussed this matter in the context of one-party consent for interception, and concluded that "(i)t is only when no party consents that the interception amounts to an interference with the right to privacy." As noted by the LRC, this approach is adopted by many comparable jurisdictions. The Canadian and Australian LRCs have looked at the issue and come to the same conclusion. We agree with the LRC's analysis in the 1996 report. The IOCO also takes this approach.

14. LEAs are given various powers by law to do things that infringe on citizens' various rights where necessary, so that LEAs can carry out their duties to protect the public. The use of such powers should be subject to different levels of checks and balances proportionate to the seriousness of the infringement. We do not consider that requiring judicial authorization for less intrusive surveillance operations (including such operations done with participant monitoring) would be the right balance. For participant monitoring, in comparable jurisdictions such as the United States and Australia, the operation requires no statutory authorization at all. We have already sought to tighten the requirement by suggesting that it be subject to executive

authorization under the law. This would bring such operations under the full range of safeguards under the proposed legislation, e.g., oversight by the Commissioner, confidentiality of documents etc. We believe that our proposal strikes the right balance between the proper use of judicial resources and the operational effectiveness of the LEAs in carrying out their duties of protecting the public.

Annex B to the Information Paper for the meeting of LegCo Panel on Security on 21 February 2006

Types of Covert Surveillance

Options for regulatory framework

In formulating our proposal for covert surveillance we have taken into account the discussion and recommendations in the 1996 consultation paper "Privacy : Regulating Surveillance and the Interception of Communications" of the Privacy Sub-Committee of the Law Reform Commission (LRC) (the 1996 LRC paper). In addition, we have taken reference from the regulatory regimes of comparable common law jurisdictions, in particular, that of Australia.

2. The **1996 LRC paper** recommends a regulatory framework comprising **three criminal offences** along these lines –

(a) entering private premises as a trespasser with intent to observe, overhear or obtain personal information therein;

(b) placing, using or servicing in, or removing from, private premises a sense-enhancing, transmitting or recording device without the consent of the lawful occupier; and

(c) placing or using a sense-enhancing, transmitting or recording device outside private premises with the intention of monitoring without the consent of the lawful occupier either the activities of the occupant or data held on the premises relating directly or indirectly to the occupant.

The 1996 LRC paper further recommends that **warrants be required to authorise** all surveillance within the scope of the proposed criminal offences.

3. On paragraph 2 (a), currently law enforcement agencies (LEAs) are already liable for trespass and any unlawful act that they may do on the premises that they have trespassed. In practice, therefore, such operations are unlawful unless authorized under the law, e.g., by way of a search warrant. Our proposed legislation corresponds to the other two proposed criminal offences in paragraph 2 above, and other situations not discussed in detail in the 1996 LRC paper.

4. The regulatory regimes of **comparable common law jurisdictions** vary considerably. The United States (US) statutory regimes cover only the use of devices to monitor and record communications. The UK's statutory regime is more up to date and comprehensive, covering intrusive surveillance (where private premises are involved) and directed surveillance (covert surveillance other than intrusive surveillance). The UK regime provides for executive authorization of directed surveillance operations and approval of executive authorizations by a Surveillance Commissioner, who must be a sitting or former judge, of intrusive surveillance operations. We have taken greater reference from the legislation Australia enacted in 2004, which is the latest model among the jurisdictions that we have studied. Previously Australia's Commonwealth legislation covered only the use of listening devices. The 2004 legislation covers listening, data surveillance, optical surveillance, and tracking devices.

Our proposed regime

Definition of covert surveillance

5. We propose that our new legislation regulates surveillance carried out for any specific investigation or operation if the surveillance is –

(a) systematic;
(b) involves the use of a surveillance device; and
(c) is –
    (i) carried out in circumstances where any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy;
    (ii) carried out in a manner calculated to ensure that the person is unaware that the surveillance is or may be taking place; and
    (iii) likely to result in the obtaining of any private information about the person.

All such surveillance would require prior authorization under the proposed new legislation.

Types of authorization required

6. As different devices capture different types of personal information, their use affects privacy in different ways. The authorization scheme seeks to take this into account.

7. ***Listening devices and data surveillance devices*** capture the content of communications, or data in or generated from data-processing equipment, which may include communication data.

8. If access to the communication is already available through the presence of a person known by the target to be accessing that information, arguably there is little intrusion into the privacy of the other parties to the conversation. For illustration, if two persons (A and B) are engaged in a conversation, and A intends to repeat the conversation to an LEA, he may do so whether he has used a device or not. B knows full well of A's presence and the possible risk of A repeating the conversation to others. In both the US and Australia, for such "participant monitoring" no warrant is required. However, for tighter protection, we propose that **where a device to pick up or record the conversation is used whilst A and B are having the conversation, and A agrees to the use of the device in his presence, the LEA would need executive authorization**.

9. If, however, A is not present at the conversation but has arranged to plant a device to pick up or record the conversation between B and C, neither B nor C would expect that their communications would be picked up by A. The intrusion into privacy in respect of B and C would be much greater (unless the conversation takes place in circumstances that do not involve a reasonable expectation of privacy on the part of B, e.g., if he shouts across the street to C when there are other parties around). **If an LEA wishes to pick up or record the private conversation through the use of a device without a participating party, that operation would need judicial authorisation**.

10. ***Optical surveillance devices and tracking devices*** capture data which are different from the oral communications captured by listening devices. As the nature of the data involved is different, the privacy analysis is different, and the authorization criteria have to be adjusted accordingly.

11. In Australia, the use of optical surveillance devices other than in circumstances involving entry onto premises without permission or interference with any vehicle or thing would not require a warrant. We propose a tighter

regime –

(a) a covert surveillance operation involving **the use of an optical surveillance device in a participant monitoring situation in places to which the public does not have access should require an executive authorization;**

(b) **the requirement for executive authorization should extend to the use of an optical surveillance device to monitor or record activities in places to which the public does not have access *provided that* such use does not involve entry onto premises or interference with the interior of a conveyance (e.g., a car) or object without permission**; and

(c) where **the use of the optical surveillance device involves entry onto premises or interference with the inside of a conveyance or object without permission, but does not involve a participant monitoring situation, judicial authorization would be required** in view of the greater intrusion.

12. For illustration, if a person (A) is in his own room and has drawn the curtains of the room, he can reasonably expect that what he does in the room would be private. If an LEA wishes to enter the room to install an optical surveillance device before the person enters that room, that operation would need judicial authorisation (paragraph 11(c) above). If, however, A allows B into the room to observe what he does, and B covertly videotapes the scene, executive authorization would be required (paragraph 11(b) above).

13. A **tracking device** captures the location data of a person or an object. The collection of such data where the person or object moves in a public place should not pose much privacy concern, since one should not have much expectation of privacy with respect to his whereabouts in a public place.

14. In Australia, the use of a tracking device not involving entry onto premises without permission or interference with the interior of a vehicle without permission requires executive authorization. Otherwise a judicial warrant is required. We propose a similar regime –

(a) **if a tracking device is used in circumstances not involving entry onto premises without permission or interference with the interior of a conveyance or object without permission, it would require executive authorization**; and

(b) **if the use of a tracking device involves entry onto premises without permission or interference with the interior of a conveyance or object without permission, the operation would require judicial authorisation** because of the greater intrusion.

15. For illustration, if a tracking device is covertly placed inside a person's briefcase in order to track his movement, judicial authorization would be required (paragraph 14(b) above). If, however, a tracking device is placed on the outside of a conveyance and may hence lead to its driver's movement being traced, it would require executive authorization (paragraph 14(a) above).

* * *