SB Ref: ICSB 17/06

Bills Committee on
Interception of Communications and Surveillance Bill

Response to issues raised at the meeting on 24 June 2006

This paper sets out the Administration's response to the issues at the Bills Committee meeting on 24 June 2006.

Clause 2(1) : Definition of "surveillance device"

- ***To consider expressly prohibiting the implantation or causing the swallowing of a surveillance device into a human body.***

2. As explained at the Bills Committee, implanting a device without the consent of the person or without express statutory authority would be unlawful. The law enforcement agencies (LEAs) do not use surveillance devices in such a way. An amendment to the Bill is not strictly necessary. However, in view of Members' suggestion, we propose to add the following CSAs to clause 30A that the Bills Committee has previously considered –

> *"(3) For the avoidance of doubt, a prescribed authorization does not authorize any device to be implanted in, or administered to, a person without the consent of the person."*

- ***To consider disallowing the use of surveillance devices which are harmful to health.***

3. We are not aware that surveillance devices using present-day technologies have harmful health effects. In any case, as explained at the Bills Committee, in many cases surveillance devices are used by LEA officers, victims and informants. It would not be in our own interest to use any surveillance device known to be harmful to health, and it is our policy not to do so. It has been our practice when acquiring new surveillance devices to take care to ensure that the devices do not have harmful health effects on either the targets of surveillance or our staff. We will continue to do so.

Clause 2(1) : Definition of "postal interception"

- ***To consider stating at the resumption of the second reading of the Bill that postal interception does not authorize putting foreign contents / objects in postal packets.***

4. As explained in our paper SB Ref. ICSB 15/06 (paragraph 16), postal interception of itself should not include replacing the contents of the communications. We have no objection to re-confirming this at the resumption of the second reading of the Bill.

Clause 2(1) : Definition of "Type 2 surveillance"

- ***To consider stipulating in the code of practice that if a Type 2 surveillance operation involves a higher level of expectation of privacy, then judge's authorization will be required.***

5. The Bill seeks to provide a clear definition of what constitutes Type 2 surveillance with objective tests. All other covert surveillance is Type 1 surveillance. We have already proposed some amendments to the definition of Type 2 surveillance in our paper SB Ref. ICSB 15/06 (paragraph 24). We consider that, with these amendments, the definition should be sufficiently clear. Nonetheless, we will require in the code of practice that LEAs should consider whether there is a higher expectation of privacy than usual in the circumstances of the case and tailor their operations accordingly.

Clause 2(2)

- ***To consider further amending clause 2(2) to clarify that "activity" does not include spoken and written words.***

6. Taking into account Members' suggestion, we have no objection to amending the proposed CSA further to make the meaning clearer, as follows –

> *"…but nothing in this subsection affects any entitlement of the person in relation to words spoken, written or read by him in a public place".*

Clause 2(1) : Definition of "telecommunications interception"

- ***To advise whether a telephone interception may also capture the***

equipment number of a mobile telephone, the location of the mobile phone, and the IP address of email messages.

7. In theory the data may be captured during an interception if it is part of the data produced in association with the communication. Whether a specific type of data is captured in a particular interception depends on the operational circumstances of the case.

Clause 3

- ***To consider further amending the proposed CSAs to provide a clearer linkage between the "purpose" and specific serious crimes or threats to public security.***
- ***To consider whether the new clause 3(1)(b)(iii) should include an express reference to the Basic Law, in particular Chapter III.***

8. As explained at the Bills Committee, the "purpose" in clause 3 has to relate to a ***specific*** serious crime or threat to public security. Hence the references "***the*** serious crime" and "***the particular*** threat to public security". In the totality of the clause and the proposed CSAs to the clause (paragraph 35 of SB Ref. ICSB 15/06), the linkage is very clear already. It would be inconceivable that an application could be made and an authorization issued for the purpose of, say, preventing or detecting serious crime without specifying what the specific serious crime to be prevented or detected is. No application of the tests of proportionality, necessity and reasonable suspicion would be possible in that case. Nonetheless, in view of a Member's concern, we have no objection to further amending the term "the serious crime" to "the ***particular*** serious crime".

9. The proposed new clause 3(1)(b)(iii) provides that in assessing the necessity and proportionality of the proposed interception or covert surveillance, the authorizing authority should consider such other matters that are relevant in the circumstances. This is a wide provision allowing the authorizing authority to take into account all matters that are relevant in the case. It does not preclude the consideration of relevant provisions of the Basic Law as appropriate. The panel judges would surely be aware of the need to take into account the relevant provisions of the Basic Law in considering applications. In the code of practice, we will remind the LEAs of the need to take into account the Basic Law. We consider

that an express reference to the Basic Law in clause 3 is not necessary.

Clause 10

- ***To re-consider amending clause 10(b) to make it clear that an authorization could cease to have effect upon a specified event.***

10. As explained at the Bills Committee, there is clear case law that the period to be specified in an authorization may be a time period or the occurrence of a specified event. We do not consider it necessary to amend the Bill in this regard. Nonetheless, in view of a Member's concern, we will remind LEAs in the code of practice that the period may include not only a time but also a specified event.

Others

- ***To bring to the Commissioner's attention that some Legislative Council Members have suggested that he may wish to collect information on the maximum duration of operations that have been renewed.***

11. We will bring this to the attention of the Commissioner.

- ***To include in the code of practice the minimum rank of the officer who may apply for authorizations.***

- ***To include in the code of practice the requirement that the applying officer cannot be the same person as the authorizing officer.***

12. We agree to the suggestions and will so provide in the code of practice.

- ***To consider providing, from impression, the rough proportion of participant monitoring cases along the lines of the statement by the judge in the Duarte case.***

13. In the Duarte case, the judge said "…… *in the United States this mode of surveillance is without question 'the most widely used and most frequently practiced [sic] mode of eavesdropping'. Though I have found no data on the relative frequency of this practice in Canada, the cases would indicate that it is also widespread here.*"

14. From our impression, participant monitoring is not the dominant mode of Type 2 surveillance.

- ***To consider stipulating, either in the code of practice or in the Bill, the arrangements for making good damage to property interfered with during an interception or covert surveillance operation and for retrieving surveillance devices after an operation as set out in paragraphs 75 to 79 of paper SB Ref. ICSB 15/06.***

15. Having reconsidered the issue, we believe that the requirements should more appropriately be set out in the code of practice than in the Bill. As set out in our paper SB Ref. ICSB 15/06, the code will require the LEAs to report to the Commissioner the remedial action that they have taken to make good the damage and, if the damage cannot be made good, the reasons. Similarly, the code will require them to report to the Commissioner all instances where they have not applied for a device retrieval warrant for devices not yet retrieved and the reasons for not doing so. Any non-compliance would be subject to review by the Commissioner.

- ***To consider, in consultation with the Judiciary, the feasibility of arranging for reviews of the decisions by the panel judges, some time (say, two years) after the establishment of the new statutory scheme, for the purpose of making recommendations to ensure consistency among panel judges and building up jurisprudence.***

16. We have consulted the Judiciary. The Judiciary has stated that it will take steps to ensure that there will be sharing of experience among panel judges (including in relation to their consideration of relevant jurisprudence) so that broad consistency in their approach may be addressed and considered by them.

Security Bureau
June 2006