

**Bills Committee on  
Interception of Communications and Surveillance Bill**

**Response to issues raised**

This paper follows up on the following points and requests for information raised at the Bills Committee since the issue of paper SB Ref : ICSB 20/06.

**(a) Committee Stage Amendments and Code of Practice**

2. The additional Committee Stage Amendments (CSAs) to which we have agreed at meetings of the Bills Committee since our paper SB Ref : ICSB 20/06 are at **Annex A**. This Annex also sets out the agreed suggestions for inclusion in the code of practice.

**(b) Clause 2(1) : definition of “serious crime” - some examples of offences that attract a maximum penalty of \$1 million or more and an imprisonment term of less than three years**

3. A relevant extract from our paper to the Security Panel on 16 February 2006 is at **Annex B**.

**(c) Clause 57 : whether records on telephone numbers and email addresses intercepted would form part of the records to be kept, and whether they will be kept under clause 57**

4. The code of practice will require LEAs to keep such records. In connection with clause 57, if the telephone numbers and email addresses are specified in the authorization, they will form part of the records to be kept under clause 57(1)(a). In rare cases of authorizations in respect of specified persons, such records will be kept under clause 57(1)(g).

**(d) Clause 60 : case law on what constitutes substantial / minor irregularity**

5. We have deposited some such cases with the Bills Committee Secretariat for Members' perusal.

**List of issues raised since paper SB Ref : ICSB 20/06**

**Agreed to by the Administration**

**COMMITTEE STAGE AMENDMENTS (CSAs) DISCUSSED WITH THE BILLS COMMITTEE**

**Clause 2(1): Definition of “copy”**

*“(a) (ii) any record referring to the interception which is a record ~~of showing, directly or indirectly,~~ the identity of any person who is the sender or intended recipient of the communication; or.....”*

**Clause 2(1): Definition of “Type 2 surveillance”**

*“(b)(ii) interference with the interior of any conveyance or object, ~~or electronic interference with the device,~~ without permission.”*

**Clause 46A(1)**

*“(1) If, in the course of performing any of his functions under this Ordinance, the Commissioner considers that there is any case in which any interception or covert surveillance has been carried out by an officer of a department without the authority of a prescribed authorization issued or renewed under this Ordinance, subject to subsection (6), the Commissioner shall as soon as reasonably practicable give notice to the relevant person .....”*

**Clause 46A(3)**

*“(3) Notwithstanding subsection (1), the Commissioner shall only give a notice under that subsection when he considers that the giving of the notice would not be prejudicial to the prevention or detection of crime or the protection of public security.”*

**Clause 47(2)(d)**

“(v) *the broad nature of recommendations made by the Commissioner under sections 48, 49 and 50 during the report period;*~~and~~”

**Clause 52**

“Without prejudice to other provisions of this Part, where the head of any department considers that there may have been any case of failure by the department or any of its officers to comply with any relevant requirement, he shall submit to the Commissioner a report with details of the case (including any disciplinary action taken in respect of any officer).”

**Clause 60**

“(1) A prescribed authorization or device retrieval warrant is not affected by any minor defect ~~in~~ relating to it.”

The same change will be made to clause 60(2).

**Schedule 2, clause 1(3)**

“(3) *The panel judge may consider the application in such manner as he considers appropriate.*”

In addition, as suggested by the Bills Committee, the original text of clause 1(1) will be reinstated and the CSA to include the proposed clause 1(4) will be dropped.

**Schedule 3**

The three references to “journalistic material” in para. (b)(viii) of Part 1 and para. (b)(ix) of Parts 2 and 3 of Schedule 3 will be amended to read as follows -

“*the likelihood that any information which may be subject to legal professional privilege, or may be the contents of any journalistic material, will be obtained by carrying out the interception;*~~and~~”

## ISSUES FOR INCLUSION IN CODE OF PRACTICE

- *To include examples of what constitutes more intrusive Type 2 surveillance that LEAs should take care in planning their operations. (raised at the meeting on 6 July 2006)*
- *To include a provision on how to deal with claims for damages from parties whose property has been interfered with in carrying out a prescribed authorization. (raised at the meeting on 8 July 2006)*
- *To set out expressly that the Commissioner may make a report to CE under clause 48 or make a recommendation to the LEA under clause 50 in respect of failure to make good damage to property in carrying out a prescribed authorization. (raised at the meeting on 8 July 2006)*
- *To explain what constitutes a “public place”. (raised at the meeting on 8 July 2006)*
- *To provide that the consent of the participating party in Type 2 surveillance should be obtained prior to the operation and this should be indicated in making the application. (raised at the meeting on 8 July 2006)*
- *To set out that the disciplinary action taken referred to in clause 46(2) includes the various stages of disciplinary actions. (raised at the meeting on 10 July 2006)*
- *To ensure that departments take appropriate steps to watch out for exculpatory material under clause 58(4). (raised at the meeting on 11 July 2006)*

**Extract of information paper for Panel on Security on 16 February 2006**

19. Apart from the imprisonment term, the level of the fine is also a good indicator of the seriousness of the offence. For example, some offences related to dutiable commodities attract a maximum penalty of imprisonment for two years and a fine of \$1 million (e.g., importing or exporting dutiable goods in contravention of the Dutiable Commodities Ordinance or forging documents required under that Ordinance). Some of these offences may involve criminal syndicates. It would, therefore, be important to ensure that, where the tests of proportionality and necessity are met, covert surveillance could be used to prevent and detect such offences.