File Ref: SBCR 3/2/3231/94

LEGISLATIVE COUNCIL BRIEF

Interception of Communications and Surveillance Bill

INTRODUCTION

At the meeting of the Executive Council on 28 February 2006, the Council ADVISED and the Chief Executive ORDERED that the Interception of Communications and Surveillance Bill, at **Annex A**, be introduced into the Legislative Council.

BACKGROUND AND ARGUMENT

Background

2. The Administration issued a paper on its legislative proposals on the regulation of interception of communications and covert surveillance (at **Annex B**) to the Panel on Security of the Legislative Council (LegCo) on 1 February 2006, and briefed the Panel as well as other interested LegCo Members on proposals at the meeting of the Panel of 7 February 2006. The background to the issues involved is set out in paragraphs 2 to 7 of that paper. The proposals were further discussed at the special meetings of the Panel on 16 February 2006 and 21 February 2006, and a further meeting of the Panel is scheduled for 2 March 2006. Our response to issues raised at the meetings are at **Annex C**.

3. Separately, on 9 February 2006, the Court of First Instance (CFI) handed down its judgment on an application for judicial review (JR) regarding the existing regime on interception of telecommunications and covert surveillance. In gist, the court –

- dismissed the declaration sought that the Chief Executive (CE) had acted in breach of his duty, and therefore unlawfully, in failing to appoint a day for the commencement of the Interception of Communications Ordinance (IOCO);

- found that the Law Enforcement (Covert Surveillance Procedures) Order (the Executive Order) made by CE in July 2005 was lawfully

made, but cannot provide lawful authority for law enforcement agencies (LEAs) to conduct covert surveillance; and

- declared that insofar as section 33 of the Telecommunications Ordinance (TO) authorizes or allows access to or disclosure of the contents of any message, it is unconstitutional.

The court recognizes that any legal vacuum brought about by the declarations made would constitute a real threat to the rule of law in Hong Kong and has therefore ordered that they be suspended for six months so as to allow time to put in place corrective legislation. The applicants for JR have appealed against the temporary validity, and the ruling in relation to the commencement of the IOCO.

The proposals

4. The Interception of Communications and Surveillance Bill ("the Bill") at **Annex A** has been prepared on the basis of the legislative proposals already presented by the Administration (the key parameters of which have been explained at the paper at **Annex B**). It follows earlier public discussions on the 1996 consultation paper of the Law Reform Commission (LRC) on interception of communications and covert surveillance, the 1996 LRC report on interception of communications, the 1997 White Bill, and the IOCO. The regime proposed in the Bill, so far as interception of communications is concerned, is very much in line with those under the LRC report and the White Bill, and we have also added improvements including additional safeguards, taking into account views that we have collected during consultations that we have done in recent months. The Bill if enacted would provide for a regime which is superior to our current regime and the alternative regimes that have so far been discussed.

5. Given the need to ensure that the LEAs may continue to conduct telecommunications interception and covert surveillance operations lawfully after the expiry of the temporary validity or if the temporary validity is successfully challenged, there is a need to process and enact the Bill as soon as possible.

OTHER OPTIONS

6. We have considered but decided against the option of bringing the IOCO into operation because, among other things, it covers only interception

and not covert surveillance and it is important to have a consistent regime covering both forms of operation. Amendments to remedy this and the IOCO's other shortcomings would have to be so extensive that the enactment of new legislation is a far better and more practicable option.

THE BILL

7. The Bill at **Annex A** provides a new legal basis for interception of communications and covert surveillance operations by the LEAs, replacing the current systems under section 33 of the TO and the Executive Order. Its object is to regulate the conduct of interception of communications and the use of surveillance devices by or on behalf of public officers. The Bill contains six Parts and five Schedules.

8. Part 1 of the Bill provides for preliminary matters such as the definitions and the conditions for the issue, renewal or continuance of prescribed authorizations.

9. Part 2 contains the prohibition provisions. It provides that no public officers shall, directly or through any other person, carry out any interception of communications or covert surveillance, unless the interception of communications or covert surveillance is carried out pursuant to a prescribed authorization, or falls under specified description.

10. Part 3 contains provisions relating to the prescribed authorizations, including the appointment of the authorizing authorities and application procedures for different types of prescribed authorizations.

11. Part 4 contains provisions relating to the Commissioner on Interception of Communications and Surveillance (the Commissioner), including his appointment and his oversight functions.

12. Part 5 provides for further safeguards in respect of interception of communications and covert surveillance carried out by departments, including the requirements for regular reviews and protection against unauthorized disclosure.

13. Part 6 contains miscellaneous provisions.

14. A more detailed description of the provisions of the Bill is at the Explanatory Memorandum of the Bill attached at **Annex A**.

LEGISLATIVE TIMETABLE

15. The legislative timetable is as follow –

Publication in the Gazette	3 March 2006
First reading and second reading	8 March 2006
Resumption of second reading and third reading	To be advised
Commencement date	Day of gazettal

IMPLICATIONS OF THE PROPOSALS

Basic Law and Human Rights Implications

16. The Bill involves specifying by law the purposes for which, and the circumstances and authority under which, LEAs may lawfully intercept communications and conduct covert surveillance involving the use of devices. It will also introduce a range of human rights safeguards. The package is in conformity with the Basic Law, including provisions concerning human rights.

Binding Effect of the Legislation

17. The Bill only seeks to provide for the authorization of interception of communications and covert surveillance operations by LEAs. It does not otherwise apply to non-Government parties or the state.

Financial and Civil Service Implications

18. The proposals to establish an authorization authority and an independent oversight authority together with a complaint mechanism involving the payment of compensation will have financial and staffing implications. The LEAs would also have to deploy resources to put in place the new system within their departments.

19. The Judiciary has expressed concern at the implications of the new legislative regime on judicial resources, and the Administration has undertaken to provide the Judiciary with the necessary additional resources.

20. We are still assessing the resource implications more fully, and will continue to do so in parallel with the discussion of the Bill with LegCo. We will try to meet the additional requirements from existing resources if possible and will seek additional resources where necessary in line with established procedures.

Other Implications

21. The proposals have no economic, sustainability, productivity or environmental implications.

PUBLIC CONSULTATION

22. We have taken into account discussions with LegCo Members and interested parties in the past months before drawing up the key parameters of our legislative proposals. A paper on the legislative proposals of the Administration (at **Annex B**) was issued to the Panel on Security on 1 February 2006. Since then, we have explained them to these interlocutors and sought their further views. Our response to the issues raised at the Panel meetings is at **Annex C**.

PUBLICITY

23. A press release will be issued on 1 March 2006. A spokesman will be available to answer any question that the press may have on the Bill.

ENQUIRIES

24. Enquiries on this brief may be directed to Mr Hubert Law, Assistant Secretary for Security, at 2810 2433.

Security Bureau
March 2006

Annex A

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE BILL

CONTENTS

Division 5 – Further Provisions Relating to Performance of Functions by Commissioner

PART 5

FURTHER SAFEGUARDS

PART 6

MISCELLANEOUS

A BILL

To

Regulate the conduct of interception of communications and the use of surveillance devices by or on behalf of public officers and to provide for related matters.

Enacted by the Legislative Council.

PART 1

PRELIMINARY

1. Short title

This Ordinance may be cited as the Interception of Communications and Surveillance Ordinance.

2. Interpretation

(1) In this Ordinance, unless the context otherwise requires –

"address" (地址), in relation to a communication transmitted by a postal service, includes a postal box address;

"authorizing officer" (授權人員), in relation to any department, means any officer designated under section 7 by the head of the department to be an authorizing officer;

"code of practice" (實務守則) means the code of practice issued under section 59;

"Commissioner" (專員) means the Commissioner on Interception of Communications and Surveillance appointed under section 38;

"communication" (通訊) means –

(*a*) any communication transmitted by a postal service; or

(*b*) any communication transmitted by a telecommunications system;

"communication transmitted by a postal service" (藉郵政服務傳送的通訊) includes a postal article;

"conduct" (行為) includes any act or omission, and any series of acts or omissions or of acts and omissions;

"conveyance" (運輸工具) means any vehicle, vessel, aircraft, hovercraft or other conveyance;

"copy" (文本) –

(*a*) in relation to any contents of a communication that have been obtained pursuant to a prescribed authorization for interception, means any of the following (whether or not in documentary form) –

(i) any copy, extract or summary of such contents which identifies itself as such copy, extract or summary of such contents;

(ii) any record referring to the interception which is a record of the identity of any person who is the sender or intended recipient of the communication; or

(*b*) in relation to any material that has been obtained pursuant to a prescribed authorization for covert surveillance, means any of the following (whether or not in documentary form) –

(i) any copy, extract or summary of the material which identifies itself as such copy, extract or summary of the material;

(ii) any transcript or record made of the material which identifies itself as such transcript or record made of the material;

"court" (法院), without prejudice to section 53 and section 4 of Schedule 2 –

(*a*) means a court as defined in section 3 of the Interpretation and General Clauses Ordinance (Cap. 1); and

(*b*) includes a magistrate and a tribunal;

"covert surveillance" (秘密監察) –

(*a*) means any systematic surveillance carried out with the use of any surveillance device for the purposes of a specific investigation or operation, if the surveillance –

(i) is carried out in circumstances where any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy;

(ii) is carried out in a manner calculated to ensure that the person is unaware that the surveillance is or may be taking place; and

(iii) is likely to result in the obtaining of any private information about the person; but

(*b*) does not include any such systematic surveillance to the extent that it constitutes interception under this Ordinance;

"data surveillance device" (數據監察器材) –

(*a*) means any device or program used to monitor or record the input of information into, or the output of information from, any information system; but

(*b*) does not include an optical surveillance device;

"department" (部門) –

(*a*) in relation to interception (including any application for the issue or renewal of a prescribed authorization for interception, any prescribed authorization for interception and any other matter relating to interception), means a department specified in Part 1 of Schedule 1;

(*b*) in relation to covert surveillance (including any application for the issue or renewal of a prescribed authorization for covert surveillance, any prescribed authorization for covert surveillance and any other matter relating to covert surveillance), means a department specified in Part 2 of Schedule 1; or

(*c*) in relation to any other matter provided for in this Ordinance, means a department specified in Part 1 or 2 of Schedule 1;

"device" (器材) includes any instrument, apparatus and equipment;

"device retrieval warrant" (器材取出手令) means a device retrieval warrant issued under section 33 (and, where the context requires, includes a device retrieval warrant to be issued under that section);

"directorate officer" (首長級人員) means an officer not below a rank equivalent to that of chief superintendent of police;

"emergency authorization" (緊急授權) means an emergency authorization issued under Division 4 of Part 3 (and, where the context requires, includes an emergency authorization to be issued under that Division);

"enhancement equipment" (增強設備), in relation to a device, means any equipment used to enhance a signal, image or other information obtained by the use of the device;

"examination" (審查) means an examination (including consideration of the application for the examination) carried out under Division 3 of Part 4 (and, where the context requires, includes such an examination to be carried out under that Division);

"executive authorization" (行政授權) means an executive authorization issued or renewed under Division 3 of Part 3 (and, where the context requires, includes an executive authorization to be issued or renewed under that Division);

"function" (職能) includes power and duty;

"head" (首長), in relation to a department, includes any deputy of the head of the department;

"information system" (資訊系統) has the meaning assigned to it by section 2(1) of the Electronic Transactions Ordinance (Cap. 553);

"inspect" (查察) includes listen to, monitor and record;

"install" (裝設) includes attach;

"intercepting act" (截取作為), 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;

"interception" (截取) –

(*a*) in relation to any communication, means the carrying out of any intercepting act in respect of the communication; or

(*b*) when appearing in a context with no specific reference to any communication, means the carrying out of any intercepting act in respect of communications;

"interception product" (截取成果) means any contents of a communication that have been obtained pursuant to a prescribed authorization for interception, and includes a copy of such contents;

"judicial authorization" (司法授權) means a judicial authorization issued or renewed under Division 2 of Part 3 (and, where the context requires, includes a judicial authorization to be issued or renewed under that Division);

"listening device" (監聽器材) –

(*a*) means any device used to overhear, listen to, monitor or record any conversation or words spoken to or by any person in conversation; but

(*b*) does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment;

"maintain" (維修), in relation to a device, includes –

(*a*) adjust, relocate, repair or service the device; and

(*b*) replace the device when it is faulty;

"optical surveillance device" (視光監察器材) –

(*a*) means any device used to record visually or observe any activity; but

(*b*) does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome the impairment;

"oral application" (口頭申請) means an oral application made under section 25(1);

"panel judge" (小組法官) means a judge appointed under section 6(1) to be a panel judge;

"postal interception" (郵件截取) means interception of any communication transmitted by a postal service;

"postal service" (郵政服務) means postal service within the meaning of the Post Office Ordinance (Cap. 98);

"premises" (處所) includes any place and, in particular, includes –

(*a*) any land or building;

(*b*) any conveyance;

(*c*) any structure (whether or not movable or offshore); and

(*d*) any part of any of the premises described in paragraph (*a*), (*b*) or (*c*);

"prescribed authorization" (訂明授權) means a judicial authorization, an executive authorization or an emergency authorization;

"protected product" (受保護成果) means any interception product or surveillance product;

"public place" (公眾地方) –

(*a*) means any premises which are a public place as defined in section 2(1) of the Summary Offences Ordinance (Cap. 228); but

(*b*) does not include any such premises to the extent that they are intended for use by members of the public as a lavatory or as a place for taking a bath or changing clothes;

"relevant authority" (有關當局) –

(*a*) in relation to an application for the issue or renewal of a judicial authorization, means the panel judge to whom the application is or has been made;

(*b*) in relation to an application for the issue or renewal of an executive authorization, means the authorizing officer to whom the application is or has been made; or

(*c*) in relation to an application for the issue of an emergency authorization, means the head of a department to whom the application is or has been made;

"relevant purpose" (有關目的), in relation to a prescribed authorization, means the purpose sought to be furthered by carrying out the interception or covert surveillance concerned as described in section 3 for the purpose of the issue or renewal, or the continuance, of the prescribed authorization;

"relevant requirement" (有關規定) means any applicable requirement under –

(*a*) any provision of this Ordinance;

(*b*) the code of practice; or

(*c*) any prescribed authorization or device retrieval warrant concerned;

"serious crime" (嚴重罪行) means any offence punishable –

(*a*) in relation to the issue or renewal, or the continuance, of a prescribed authorization for interception, by a maximum

penalty that is or includes a term of imprisonment of not less than 7 years; or

(*b*) in relation to the issue or renewal, or the continuance, of a prescribed authorization for covert surveillance, by a maximum penalty that is or includes –

(i) a term of imprisonment of not less than 3 years; or

(ii) a fine of not less than $1,000,000;

"surveillance device" (監察器材) means –

(*a*) a data surveillance device, a listening device, an optical surveillance device or a tracking device;

(*b*) a device that is a combination of any 2 or more of the devices referred to in paragraph (*a*); or

(*c*) a device of a class prescribed by regulation made under section 62 for the purposes of this definition;

"surveillance product" (監察成果) means any material obtained pursuant to a prescribed authorization for covert surveillance, and includes a copy of the material;

"telecommunications interception" (電訊截取) means interception of any communication transmitted by a telecommunications system;

"telecommunications service" (電訊服務) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

"telecommunications system" (電訊系統) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

"tracking device" (追蹤器材) means any electronic device used to determine or monitor the location of any person or any object or the status of any object;

"transmitted" (傳送) includes being transmitted;

"Type 1 surveillance" (第1類監察) means any covert surveillance other than Type 2 surveillance;

"Type 2 surveillance" (第 2 類監察), subject to subsection (3), means any covert surveillance to the extent that –

(*a*) it is carried out with the use of a surveillance device for any purpose involving listening to, monitoring or recording words spoken or activity carried out by any person, and the person using the device is one –

(i) who –

(A) is the person speaking or carrying out the words or activity; or

(B) is a person, or is included in a class of persons, by whom the person described in sub-subparagraph (A) intends, or should reasonably expect, the words or activity to be heard or seen; or

(ii) who listens to, monitors or records the words or activity with the consent, express or implied, of a person described in subparagraph (i)(A) or (B); or

(*b*) it is carried out with the use of an optical surveillance device or a tracking device and the use of the device does not involve –

(i) entry onto any premises without permission; or

(ii) interference with the interior of any conveyance or object without permission.

(2) For the purposes of this 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.

(3) For the purposes of this Ordinance, any covert surveillance which is Type 2 surveillance under the definition of "Type 2 surveillance" in subsection (1) is regarded as Type 1 surveillance if it is likely that any

information which may be subject to legal professional privilege will be obtained by carrying it out.

(4) For the purposes of this Ordinance –

(*a*) a communication transmitted by a postal service is regarded as being in the course of the transmission if it is regarded as being in course of transmission by post under section 2(2) of the Post Office Ordinance (Cap. 98); and

(*b*) a communication transmitted by a telecommunications system is not regarded as being in the course of the transmission if it has been received by the intended recipient of the communication or by an information system or facility under his control or to which he may have access, whether or not he has actually read or listened to the contents of the communication.

(5) For the purposes of this Ordinance, the contents of any communication transmitted by a telecommunications system include any data produced in association with the communication.

(6) For the purposes of this Ordinance –

(*a*) an application is also regarded as being made orally if it is made by telephone, video conferencing or other electronic means by which words spoken can be heard (whether or not any part of the application is made in writing);

(*b*) information is also regarded as being provided orally if it is provided by telephone, video conferencing or other electronic means by which words spoken can be heard (whether or not any part of the information is provided in writing); and

(*c*) a determination (including the issue of a prescribed authorization or a renewed prescribed authorization and the giving of any reason) is also regarded as being

delivered orally if it is delivered by telephone, video conferencing or other electronic means by which words spoken can be heard (whether or not any part of the determination is delivered in writing).

(7) Without prejudice to section 54 of the Interpretation and General Clauses Ordinance (Cap. 1), any reference in this Ordinance to a panel judge or any officer of a department (however expressed) includes –

(*a*) where the person who has been such panel judge or officer is no longer holding office as such panel judge or officer, the person for the time being holding such office or appointed to act in or perform the functions of such office or lawfully performing the functions of such office; or

(*b*) where the person who is such panel judge or officer is unable to perform the functions of the office of such panel judge or officer, the person for the time being appointed to act in or perform the functions of such office or lawfully performing the functions of such office.

3. Conditions for issue, renewal or continuance of prescribed authorization

(1) In this Ordinance, the conditions for the issue or renewal, or the continuance, of a prescribed authorization, are that, in the circumstances of the particular case –

(*a*) the purpose sought to be furthered by carrying out the interception or covert surveillance concerned is that of –

(i) preventing or detecting serious crime; or

(ii) protecting public security; and

(*b*) the interception or covert surveillance is proportionate to the purpose sought to be furthered by carrying it out, upon –

(i) balancing, in operational terms, the relevant factors against the intrusiveness of the interception or covert surveillance on any person who is to be the subject of or may be affected by the interception or covert surveillance; and

(ii) considering whether the purpose sought to be furthered by carrying out the interception or covert surveillance can reasonably be furthered by other less intrusive means.

(2) In this section, "relevant factors" (有關因素) means –

(*a*) the immediacy and gravity of –

(i) where the purpose sought to be furthered by carrying out the interception or covert surveillance concerned is that specified in subsection (1)(*a*)(i), the serious crime to be prevented or detected; or

(ii) where the purpose sought to be furthered by carrying out the interception or covert surveillance concerned is that specified in subsection (1)(*a*)(ii), the particular threat to public security; and

(*b*) the likely value and relevance, in relation to the purpose sought to be furthered by carrying out the interception or covert surveillance, of the information likely to be obtained by carrying it out.

PART 2

PROHIBITION ON INTERCEPTION AND COVERT SURVEILLANCE

4. Prohibition on interception

(1) Subject to subsection (2), no public officer shall, directly or through any other person, carry out any interception.

(2) Subsection (1) does not apply to –

(*a*) any interception carried out pursuant to a prescribed authorization;

(*b*) any interception of telecommunications transmitted by radiocommunications (other than the radiocommunications part of a telecommunications network for the provision of a public telecommunications service by any carrier licensee under the Telecommunications Ordinance (Cap. 106)); and

(*c*) any interception authorized, permitted or required to be carried out by or under any enactment other than this Ordinance (including any interception carried out in the course of the execution of an order of a court authorizing the search of any premises or the seizure of any evidence).

(3) In this section, "carrier licensee" (傳送者牌照持有人), "public telecommunications service" (公共電訊服務), "radiocommunications" (無線電通訊), "telecommunications" (電訊) and "telecommunications network" (電訊網絡) have the meanings respectively assigned to them by section 2(1) of the Telecommunications Ordinance (Cap. 106).

5. Prohibition on covert surveillance

(1) Subject to subsection (2), no public officer shall, directly or through any other person, carry out any covert surveillance.

(2) Subsection (1) does not apply to any covert surveillance carried out pursuant to a prescribed authorization.

PART 3

PRESCRIBED AUTHORIZATIONS, ETC.

Division 1 – Relevant Authorities

6. Panel judges

(1) The Chief Executive shall, on the recommendation of the Chief Justice, appoint 3 to 6 eligible judges to be panel judges for the purposes of this Ordinance.

(2) A panel judge shall be appointed for a period of 3 years, and may from time to time be reappointed.

(3) The Chief Executive may, on the recommendation of the Chief Justice, revoke the appointment of a panel judge for good cause.

(4) Schedule 2 applies to and in relation to the procedures of, and other matters relating to, a panel judge.

(5) In this section, "eligible judge" (合資格法官) means a judge of the Court of First Instance.

7. Authorizing officers

The head of a department may designate any officer not below a rank equivalent to that of senior superintendent of police to be an authorizing officer for the purposes of this Ordinance.

Division 2 – Judicial Authorizations

Issue of judicial authorizations

8. Application for judicial authorization for interception or Type 1 surveillance

(1) An officer of a department may apply to a panel judge for the issue of a judicial authorization for any interception or Type 1 surveillance to be carried out by or on behalf of any of the officers of the department.

(2) The application is –

(*a*) to be made in writing; and

(*b*) to be supported by an affidavit of the applicant which is to comply with the requirements specified in –

(i) in the case of a judicial authorization for interception, Part 1 of Schedule 3; or

(ii) in the case of a judicial authorization for Type 1 surveillance, Part 2 of Schedule 3.

(3) An application may not be made under subsection (1) unless the making of the application has been approved by a directorate officer of the department concerned.

9. Determination of application for judicial authorization

(1) Upon considering an application for the issue of a judicial authorization made under section 8, the panel judge may, subject to subsection (2) –

(*a*) issue the judicial authorization sought under the application, with or without variations; or

(*b*) refuse to issue the judicial authorization.

(2) The panel judge shall not issue the judicial authorization unless he is satisfied that the conditions for its issue under section 3 have been met.

(3) The panel judge shall deliver his determination under subsection (1) by –

(*a*) in the case of subsection (1)(*a*), issuing the judicial authorization in writing; or

(*b*) in the case of subsection (1)(*b*), giving the reason for the refusal in writing.

10. Duration of judicial authorization

A judicial authorization –

(*a*) takes effect at the time specified by the panel judge when issuing the judicial authorization, which in any case is not to be earlier than the time when it is issued; and

(*b*) subject to any renewal under this Division, ceases to have effect upon the expiration of the period specified by the panel judge when issuing the judicial authorization, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Renewal of judicial authorizations

11. Application for renewal of judicial authorization

(1) At any time before a judicial authorization ceases to have effect, an officer of the department concerned may apply to a panel judge for the renewal of the judicial authorization.

(2) The application is –

(*a*) to be made in writing; and

(*b*) to be supported by –

(i) a copy of the judicial authorization sought to be renewed;

(ii) a copy of any affidavit provided under this Part for the purposes of any application for the issue or renewal of the judicial authorization, or for the purposes of any application made further to an oral application for confirmation of the judicial authorization or its previous renewal; and

(iii) an affidavit of the applicant which is to comply with the requirements specified in Part 4 of Schedule 3.

(3) An application may not be made under subsection (1) unless the making of the application has been approved by a directorate officer of the department concerned.

12. Determination of application for renewal of judicial authorization

(1) Upon considering an application for the renewal of a judicial authorization made under section 11, the panel judge may, subject to subsection (2) –

(*a*) grant the renewal sought under the application, with or without variations; or

(*b*) refuse to grant the renewal.

(2) The panel judge shall not grant the renewal unless he is satisfied that the conditions for its grant under section 3 have been met.

(3) The panel judge shall deliver his determination under subsection (1) by –

(*a*) in the case of subsection (1)(*a*), issuing the renewed judicial authorization in writing; or

(*b*) in the case of subsection (1)(*b*), giving the reason for the refusal in writing.

(4) A judicial authorization may be renewed more than once under this Ordinance.

13. Duration of renewal of judicial authorization

A renewal of a judicial authorization –

(*a*) takes effect at the time when the judicial authorization would have ceased to have effect but for the renewal; and

(*b*) subject to any further renewal under this Division, ceases to have effect upon the expiration of the period specified by the panel judge when granting the renewal, which in

any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Division 3 – Executive Authorizations

Issue of executive authorizations

14. Application for executive authorization for Type 2 surveillance

(1) An officer of a department may apply to an authorizing officer of the department for the issue of an executive authorization for any Type 2 surveillance to be carried out by or on behalf of any of the officers of the department.

(2) The application is –

(*a*) to be made in writing; and

(*b*) to be supported by a statement in writing made by the applicant which is to comply with the requirements specified in Part 3 of Schedule 3.

15. Determination of application for executive authorization

(1) Upon considering an application for the issue of an executive authorization made under section 14, the authorizing officer may, subject to subsection (2) –

(*a*) issue the executive authorization sought under the application, with or without variations; or

(*b*) refuse to issue the executive authorization.

(2) The authorizing officer shall not issue the executive authorization unless he is satisfied that the conditions for its issue under section 3 have been met.

(3) The authorizing officer shall deliver his determination under subsection (1) by –

(*a*) in the case of subsection (1)(*a*), issuing the executive authorization in writing; or

(*b*) in the case of subsection (1)(*b*), giving the reason for the refusal in writing.

16. Duration of executive authorization

An executive authorization –

(*a*) takes effect at the time specified by the authorizing officer when issuing the executive authorization, which in any case is not to be earlier than the time when it is issued; and

(*b*) subject to any renewal under this Division, ceases to have effect upon the expiration of the period specified by the authorizing officer when issuing the executive authorization, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Renewal of executive authorizations

17. Application for renewal of executive authorization

(1) At any time before an executive authorization ceases to have effect, an officer of the department concerned may apply to an authorizing officer of the department for the renewal of the executive authorization.

(2) The application is –

(*a*) to be made in writing; and

(*b*) to be supported by –

(i) a copy of the executive authorization sought to be renewed;

(ii) a copy of any statement provided under this Part for the purposes of any application for the issue or renewal of the executive authorization, or for the

purposes of any application made further to an oral application for confirmation of the executive authorization or its previous renewal; and

(iii) a statement in writing made by the applicant which is to comply with the requirements specified in Part 4 of Schedule 3.

18. Determination of application for renewal of executive authorization

(1) Upon considering an application for the renewal of an executive authorization made under section 17, the authorizing officer may, subject to subsection (2) –

(*a*) grant the renewal sought under the application, with or without variations; or

(*b*) refuse to grant the renewal.

(2) The authorizing officer shall not grant the renewal unless he is satisfied that the conditions for its grant under section 3 have been met.

(3) The authorizing officer shall deliver his determination under subsection (1) by –

(*a*) in the case of subsection (1)(*a*), issuing the renewed executive authorization in writing; or

(*b*) in the case of subsection (1)(*b*), giving the reason for the refusal in writing.

(4) An executive authorization may be renewed more than once under this Ordinance.

19. Duration of renewal of executive authorization

A renewal of an executive authorization –

(*a*) takes effect at the time when the executive authorization would have ceased to have effect but for the renewal; and

(*b*) subject to any further renewal under this Division, ceases to have effect upon the expiration of the period specified by the authorizing officer when granting the renewal, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Division 4 – Emergency Authorizations

Issue of emergency authorizations

20. Application for emergency authorization for interception or Type 1 surveillance in case of emergency

(1) An officer of a department may apply to the head of the department for the issue of an emergency authorization for any interception or Type 1 surveillance to be carried out by or on behalf of any of the officers of the department, if he considers that –

(*a*) there is immediate need for the interception or Type 1 surveillance to be carried out by reason of an imminent risk of –

(i) death or serious bodily harm of any person;

(ii) substantial damage to property;

(iii) serious threat to public security; or

(iv) loss of vital evidence; and

(*b*) having regard to all the circumstances of the case, it is not reasonably practicable to apply for the issue of a judicial authorization for the interception or Type 1 surveillance.

(2) The application is –

(*a*) to be made in writing; and

(*b*) to be supported by a statement in writing made by the applicant which is to –

(i) set out the reason for making the application; and

(ii) comply with –

(A) in the case of an emergency authorization for interception, the requirements specified in Part 1 of Schedule 3 which are to apply to the statement as they apply to an affidavit referred to in section 8(2)(*b*); or

(B) in the case of an emergency authorization for Type 1 surveillance, the requirements specified in Part 2 of Schedule 3 which are to apply to the statement as they apply to an affidavit referred to in section 8(2)(*b*).

21. Determination of application for emergency authorization

(1) Upon considering an application for the issue of an emergency authorization made under section 20, the head of the department concerned may, subject to subsection (2) –

(*a*) issue the emergency authorization sought under the application, with or without variations; or

(*b*) refuse to issue the emergency authorization.

(2) The head of the department shall not issue the emergency authorization unless he is satisfied –

(*a*) that section 20(1)(*a*) and (*b*) applies; and

(*b*) that the conditions for the issue of the emergency authorization under section 3 have been met.

(3) The head of the department shall deliver his determination under subsection (1) by –

(*a*) in the case of subsection (1)(*a*), issuing the emergency authorization in writing; or

(*b*) in the case of subsection (1)(*b*), giving the reason for the refusal in writing.

22. Duration of emergency authorization

(1) An emergency authorization –

(*a*) takes effect at the time specified by the head of the department concerned when issuing the emergency authorization, which in any case is not to be earlier than the time when it is issued; and

(*b*) ceases to have effect upon the expiration of the period specified by the head of the department when issuing the emergency authorization, which in any case is not to be longer than the period of 48 hours beginning with the time when it takes effect.

(2) Without prejudice to any application under section 8 for the issue of any judicial authorization for the interception or Type 1 surveillance concerned, an emergency authorization may not be renewed under this Ordinance.

Application for confirmation of emergency authorizations

23. Application for confirmation of emergency authorization

(1) Where any interception or Type 1 surveillance is carried out pursuant to an emergency authorization, the head of the department concerned shall cause an officer of the department to apply to a panel judge for confirmation of the emergency authorization, as soon as reasonably practicable after, and in any event within the period of 48 hours beginning with, the time when the emergency authorization takes effect.

(2) The application is –

(*a*) to be made in writing; and

(*b*) to be supported by –

(i) a copy of the emergency authorization; and

(ii) an affidavit of the applicant which is to verify the contents of the statement provided under section 20(2)(*b*) for the purposes of the application for the issue of the emergency authorization.

(3) If no application for confirmation of the emergency authorization is made within the period of 48 hours referred to in subsection (1), the head of the department concerned shall –

(*a*) cause the immediate destruction of any information obtained by carrying out the interception or Type 1 surveillance concerned, to the extent that it could not have been obtained without carrying out the interception or Type 1 surveillance; and

(*b*) without prejudice to section 52, submit to the Commissioner a report with details of the case.

24. Determination of application for confirmation of emergency authorization

(1) Upon considering an application for confirmation of an emergency authorization as provided for in section 23(1), the panel judge may, subject to subsection (2) –

(*a*) confirm the emergency authorization; or

(*b*) refuse to confirm the emergency authorization.

(2) The panel judge shall not confirm the emergency authorization unless he is satisfied that section 21(2)(*b*) has been complied with in the issue of the emergency authorization.

(3) Where the panel judge refuses to confirm the emergency authorization under subsection (1)(*b*), he may make one or more of the following orders –

(*a*) in any case where the emergency authorization still has effect at the time of the determination, an order that the

emergency authorization is, notwithstanding any other provision of this Ordinance –

(i) to be revoked upon the making of the determination; or

(ii) only to have effect subject to the variations specified by him, from the time of the determination;

(*b*) in any case whether or not the emergency authorization still has effect at the time of the determination, an order that the head of the department concerned shall cause the immediate destruction of any information obtained by carrying out the interception or Type 1 surveillance concerned, to the extent –

(i) subject to subparagraph (ii), that it could not have been obtained without carrying out the interception or Type 1 surveillance; or

(ii) where paragraph (*a*)(ii) applies, that is specified in the order.

(4) Where the emergency authorization is revoked under subsection (3)(*a*)(i), the emergency authorization is, notwithstanding section 22(1)(*b*), to cease to have effect from the time of the revocation.

(5) The panel judge shall deliver his determination under subsection (1) by –

(*a*) in the case of subsection (1)(*a*), endorsing his confirmation on the emergency authorization in writing; or

(*b*) in the case of subsection (1)(*b*), giving the reason for the refusal and making any order under subsection (3) in writing.

Division 5 – Special Provisions for Oral Applications

Oral applications

25. Oral application and its effect

(1) Notwithstanding the relevant written application provision, an application for the issue or renewal of a prescribed authorization under this Ordinance may be made orally, if the applicant considers that, having regard to all the circumstances of the case, it is not reasonably practicable to make the application in accordance with the relevant written application provision.

(2) Notwithstanding the relevant determination provision and without prejudice to the relevant conditions provision, where an oral application is made, the relevant authority shall not issue or grant the prescribed authorization or renewal sought under the application unless he is satisfied that, having regard to all the circumstances of the case, it is not reasonably practicable to make the application in accordance with the relevant written application provision.

(3) Notwithstanding the relevant document provision, where an oral application is made, the information required to be provided for the purposes of the application under the relevant document provision may be provided orally (and accordingly any requirement as to the making of any affidavit or statement does not apply).

(4) Notwithstanding the relevant written determination provision, where an oral application is made, the relevant authority may deliver the determination required to be delivered in respect of the application under the relevant determination provision by –

(*a*) issuing the prescribed authorization or the renewed prescribed authorization orally; or

(*b*) where he refuses to issue or grant the prescribed authorization or renewal sought under the application, giving the reason for the refusal orally.

(5) Except as otherwise provided in this Division, any oral application and any prescribed authorization or renewal issued or granted as a result of that application are for all purposes regarded as having the same effect respectively as an application made in writing and a prescribed authorization or renewal issued or granted as a result of that application, and the provisions of this Ordinance are, subject to necessary modifications, to apply accordingly.

(6) In this section –

"relevant conditions provision" (有關條件條文) means section 9(2), 12(2), 15(2), 18(2) or 21(2) (as may be applicable);

"relevant determination provision" (有關決定條文) means section 9(1), 12(1), 15(1), 18(1) or 21(1) (as may be applicable);

"relevant document provision" (有關文件條文) means section 8(2)(*b*), 11(2)(*b*), 14(2)(*b*), 17(2)(*b*) or 20(2)(*b*) (as may be applicable);

"relevant written application provision" (有關書面申請條文) means section 8(2)(*a*), 11(2)(*a*), 14(2)(*a*), 17(2)(*a*) or 20(2)(*a*) (as may be applicable);

"relevant written determination provision" (有關書面決定條文) means section 9(3), 12(3), 15(3), 18(3) or 21(3) (as may be applicable).

Application for confirmation of prescribed authorizations or renewals issued or granted upon oral applications

26. Application for confirmation of prescribed authorization or renewal issued or granted upon oral application

(1) Where, as a result of an oral application, the prescribed authorization or renewal sought under the application has been issued or granted, the head of the department concerned shall cause an officer of the department to apply to the relevant authority for confirmation of the prescribed authorization or renewal, as soon as reasonably practicable after, and in any event within the period of 48 hours beginning with, the time when the prescribed authorization or renewal takes effect.

(2) The application is –

(*a*) to be made in writing; and

(*b*) to be supported by –

(i) a record in writing containing all the information that would have been provided to the relevant authority in writing under the relevant written application provision had the oral application been made in writing;

(ii) where section 25(3) applies in relation to the oral application –

(A) where the relevant authority is a panel judge, an affidavit of the applicant which is to verify all the information provided pursuant to that section for the purposes of the oral application; or

(B) where the relevant authority is not a panel judge, a statement in writing made by the applicant setting out all the information provided pursuant to that section for the purposes of the oral application; and

(iii) where section 25(4) applies in relation to the oral application, a record in writing setting out the determination delivered pursuant to that section in respect of the oral application.

(3) If no application for confirmation of the prescribed authorization or renewal is made within the period of 48 hours referred to in subsection (1), then –

(*a*) in any case where the prescribed authorization or renewal still has effect upon the expiration of the period, the prescribed authorization or renewal is, notwithstanding

any other provision of this Ordinance, to be regarded as revoked upon the expiration of the period; and

(*b*) in any case whether or not the prescribed authorization or renewal still has effect upon the expiration of the period, the head of the department concerned shall –

(i) cause the immediate destruction of any information obtained by carrying out the interception or covert surveillance concerned, to the extent that it could not have been obtained without carrying out the interception or covert surveillance; and

(ii) without prejudice to section 52, submit to the Commissioner a report with details of the case.

(4) Where the prescribed authorization or renewal is regarded as revoked under subsection (3)(*a*), the prescribed authorization or renewal is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.

(5) In this section –

"relevant duration provision" (有關時限條文) means section 10(*b*), 13(*b*), 16(*b*) or 19(*b*) (as may be applicable);

"relevant written application provision" (有關書面申請條文) means section 8(2)(*a*), 11(2)(*a*), 14(2)(*a*), 17(2)(*a*) or 20(2)(*a*) (as may be applicable).

27. Determination of application for confirmation of prescribed authorization or renewal issued or granted upon oral application

(1) Upon considering an application for confirmation of a prescribed authorization or renewal as provided for in section 26(1), the relevant authority may, subject to subsection (2) –

(*a*) confirm the prescribed authorization or renewal; or

(*b*) refuse to confirm the prescribed authorization or renewal.

(2) The relevant authority shall not confirm the prescribed authorization or renewal unless he is satisfied that the relevant conditions provision has been complied with in the issue or grant of the prescribed authorization or renewal.

(3) Where the relevant authority refuses to confirm the prescribed authorization or renewal under subsection (1)(*b*), he may make one or more of the following orders –

(*a*) in any case where the prescribed authorization or renewal still has effect at the time of the determination, an order that the prescribed authorization or renewal is, notwithstanding any other provision of this Ordinance –

(i) to be revoked upon the making of the determination; or

(ii) only to have effect subject to the variations specified by him, from the time of the determination;

(*b*) in any case whether or not the prescribed authorization or renewal still has effect at the time of the determination, an order that the head of the department concerned shall cause the immediate destruction of any information obtained by carrying out the interception or covert surveillance concerned, to the extent –

(i) subject to subparagraph (ii), that it could not have been obtained without carrying out the interception or covert surveillance; or

(ii) where paragraph (*a*)(ii) applies, that is specified in the order.

(4) Where the prescribed authorization or renewal is revoked under subsection (3)(*a*)(i), the prescribed authorization or renewal is, notwithstanding

the relevant duration provision, to cease to have effect from the time of the revocation.

(5) The relevant authority shall deliver his determination under subsection (1) by –

(*a*) in the case of subsection (1)(*a*), issuing the prescribed authorization or the renewed prescribed authorization (being the prescribed authorization confirmed under that subsection or being in terms of the renewal confirmed under that subsection (as the case may be)) in writing; or

(*b*) in the case of subsection (1)(*b*), giving the reason for the refusal and making any order under subsection (3) in writing.

(6) In this section –

"relevant conditions provision" (有關條件條文) means section 9(2), 12(2), 15(2), 18(2) or 21(2)(*b*) (as may be applicable);

"relevant duration provision" (有關時限條文) means section 10(*b*), 13(*b*), 16(*b*), 19(*b*) or 22(1)(*b*) (as may be applicable).

28. Special case of emergency authorization issued as a result of oral application

(1) Where an emergency authorization is issued as a result of an oral application, sections 26 and 27 do not apply if –

(*a*) an application for confirmation of the emergency authorization as provided for in section 23(1) has been made to a panel judge within the period of 48 hours referred to in that section; and

(*b*) the application is supported by –

(i) a record referred to in section 26(2)(*b*)(i);

(ii) an affidavit of the applicant which is to verify the contents of the statement provided under section

20(2)(*b*) for the purposes of the application for the issue of the emergency authorization or, where section 25(3) applies in relation to the oral application, all the information provided pursuant to section 25(3) for the purposes of the oral application; and

(iii) a copy of the emergency authorization or, where section 25(4) applies in relation to the oral application, a record in writing setting out the determination delivered pursuant to that section in respect of the oral application.

(2) Notwithstanding section 23(2)(*b*), the application described in subsection (1)(*a*) and (*b*) is for all purposes regarded as an application duly made for confirmation of the emergency authorization as provided for in section 23(1), and the provisions of this Ordinance are to apply accordingly (subject to section 24(5)(*a*) being read as requiring the panel judge to deliver his determination under section 24(1) by issuing the emergency authorization (being the emergency authorization confirmed under section 24(1)(*a*)) in writing).

Division 6 – General Provisions for Prescribed Authorizations

Matters authorized, required or provided for by prescribed authorizations

29. What a prescribed authorization may authorize or require under or by virtue of its terms, etc.

(1) A prescribed authorization for interception may –

(*a*) in the case of a postal interception, contain terms that authorize one or both of the following –

(i) the interception of communications made to or from any premises or address specified in the prescribed authorization;

(ii) the interception of communications made to or by any person specified in the prescribed authorization (whether by name or by description); or

(*b*) in the case of a telecommunications interception, contain terms that authorize one or both of the following –

(i) the interception of communications made to or from any telecommunications service specified in the prescribed authorization;

(ii) the interception of communications made to or from any telecommunications service that any person specified in the prescribed authorization (whether by name or by description) is using, or is likely to use.

(2) A prescribed authorization for covert surveillance may contain terms that authorize one or more of the following –

(*a*) the use of any surveillance devices in or on any premises specified in the prescribed authorization;

(*b*) the use of any surveillance devices in or on any object or class of objects specified in the prescribed authorization;

(*c*) the use of any surveillance devices in respect of the conversations, activities or location of any person specified in the prescribed authorization (whether by name or by description).

(3) A prescribed authorization, other than an executive authorization, may contain terms that authorize the doing of anything reasonably necessary to

conceal any conduct authorized or required to be carried out under the prescribed authorization.

(4) A prescribed authorization, other than an executive authorization, may, if it is necessary for the execution of the prescribed authorization, contain terms that authorize the interference with any property (whether or not of any person who is the subject of the interception or covert surveillance concerned).

(5) A prescribed authorization, other than an executive authorization, may contain terms that require any person specified in the prescribed authorization (whether by name or by description), on being shown a copy of the prescribed authorization, to provide to any of the officers of the department concerned such assistance in the execution of the prescribed authorization as is specified in the prescribed authorization.

(6) A prescribed authorization for interception also authorizes –

(*a*) the installation, use and maintenance of any devices required to be used in order to intercept any of the communications authorized to be intercepted under the prescribed authorization;

(*b*) the entry, by force if necessary, onto any premises in order to carry out any conduct authorized or required to be carried out under the prescribed authorization;

(*c*) the interception of any communication which it is necessary to intercept in order to intercept any of the communications authorized to be intercepted under the prescribed authorization; and

(*d*) where subsection (1)(*a*)(ii) or (*b*)(ii) is applicable, the provision to any person, for the execution of the prescribed authorization, of particulars of the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying –

(i) in the case of subsection (1)(*a*)(ii), the communications made to or by the person specified in the prescribed authorization; or

(ii) in the case of subsection (1)(*b*)(ii), the communications made to or from any telecommunications service that the person specified in the prescribed authorization is using, or is likely to use.

(7) A prescribed authorization for covert surveillance also authorizes –

(*a*) where subsection (2)(*a*) is applicable –

(i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization in or on the premises specified in the prescribed authorization; and

(ii) the entry, by force if necessary, onto the premises, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization;

(*b*) where subsection (2)(*b*) is applicable –

(i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization in or on the object, or an object of the class, specified in the prescribed authorization; and

(ii) the entry, by force if necessary, onto any premises where the object, or an object of the class, is reasonably believed to be or likely to be, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct

authorized or required to be carried out under the prescribed authorization; and

(*c*) where subsection (2)(*c*) is applicable –

(i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization, in or on any premises where the person specified in the prescribed authorization is reasonably believed to be or likely to be; and

(ii) the entry, by force if necessary, onto the premises, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization.

30. What a prescribed authorization further authorizes

A prescribed authorization further authorizes the undertaking of any conduct which it is necessary to undertake in order to carry out what is authorized or required to be carried out under the prescribed authorization and, without limiting the generality of the foregoing, such conduct includes –

(*a*) the retrieval of any of the devices authorized to be used under the prescribed authorization;

(*b*) the installation, use, maintenance and retrieval of any enhancement equipment for the devices;

(*c*) the temporary removal of any conveyance or object from any premises for the installation, maintenance or retrieval of the devices or enhancement equipment and the return of the conveyance or object to the premises;

(*d*) the breaking open of anything for the installation, maintenance or retrieval of the devices or enhancement equipment;

(*e*) the connection of the devices or enhancement equipment to any source of electricity and the use of electricity from that source to operate the devices or enhancement equipment;

(*f*) the connection of the devices or enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the devices or enhancement equipment; and

(*g*) the provision of assistance for the execution of the prescribed authorization.

31. Prescribed authorization may be issued or renewed subject to conditions

A prescribed authorization may be issued or renewed subject to any conditions specified in it that apply to the prescribed authorization itself or to any further authorization or requirement under it (whether granted or imposed under its terms or any provision of this Ordinance).

Device retrieval warrants after prescribed authorizations having ceased to have effect

32. Application for device retrieval warrant

(1) Where a prescribed authorization has in any way ceased to have effect under this Ordinance, an officer of the department concerned may apply to a panel judge for the issue of a device retrieval warrant authorizing the retrieval of any of the devices authorized to be used under the prescribed authorization if such devices –

(*a*) have been installed in or on any premises or object, pursuant to the prescribed authorization; and

(*b*) are still in or on such premises or object, or are in or on any other premises or object.

(2) The application is –

(*a*) to be made in writing; and

(*b*) to be supported by –

(i) a copy of the prescribed authorization; and

(ii) an affidavit of the applicant which is to comply with the requirements specified in Schedule 4.

33. Determination of application for device retrieval warrant

(1) Upon considering an application for the issue of a device retrieval warrant made under section 32, the panel judge may, subject to subsection (2) –

(*a*) issue the device retrieval warrant sought under the application, with or without variations; or

(*b*) refuse to issue the device retrieval warrant.

(2) The panel judge shall not issue the device retrieval warrant unless he is satisfied that section 32(1)(*a*) and (*b*) applies to the devices concerned.

(3) The panel judge shall deliver his determination under subsection (1) by –

(*a*) in the case of subsection (1)(*a*), issuing the device retrieval warrant in writing; or

(*b*) in the case of subsection (1)(*b*), giving the reason for the refusal in writing.

34. Duration of device retrieval warrant

A device retrieval warrant –

(*a*) takes effect at the time specified by the panel judge when issuing the warrant, which in any case is not to be earlier than the time when it is issued; and

(*b*) ceases to have effect upon the expiration of the period specified by the panel judge when issuing the warrant, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

35. What a device retrieval warrant may authorize under or by virtue of its terms, etc.

(1) A device retrieval warrant may authorize the retrieval of any devices specified in the warrant.

(2) A device retrieval warrant may contain terms that authorize the doing of anything reasonably necessary to conceal any conduct authorized to be carried out under the warrant.

(3) A device retrieval warrant may, if it is necessary for the execution of the warrant, contain terms that authorize the interference with any property (whether or not of any person who is the subject of the interception or covert surveillance concerned).

36. What a device retrieval warrant further authorizes

(1) A device retrieval warrant further authorizes the undertaking of any conduct which it is necessary to undertake in order to carry out what is authorized to be carried out under the warrant and, without limiting the generality of the foregoing, such conduct includes –

(*a*) the retrieval of any enhancement equipment for the devices authorized to be retrieved under the warrant;

(*b*) the entry, by force if necessary, onto any premises where the devices or enhancement equipment are reasonably believed to be or likely to be, and onto any other premises

adjoining or providing access to the premises, in order to retrieve the devices or enhancement equipment;

(*c*) the temporary removal of any conveyance or object from any premises for the retrieval of the devices or enhancement equipment and the return of the conveyance or object to the premises;

(*d*) the breaking open of anything for the retrieval of the devices or enhancement equipment; and

(*e*) the provision of assistance for the execution of the warrant.

(2) A device retrieval warrant which authorizes the retrieval of any tracking devices also authorizes the use of the tracking devices and any enhancement equipment for the tracking devices solely for the purposes of the location and retrieval of the tracking devices or enhancement equipment.

37. Device retrieval warrant may be issued subject to conditions

A device retrieval warrant may be issued subject to any conditions specified in it that apply to the warrant itself or to any further authorization under it (whether granted under its terms or any provision of this Ordinance).

PART 4

THE COMMISSIONER

Division 1 – The Commissioner and his Functions

38. The Commissioner

(1) There is hereby established an office by the name of the Commissioner on Interception of Communications and Surveillance.

(2) The Chief Executive shall, on the recommendation of the Chief Justice, appoint an eligible judge to be the Commissioner.

(3) The Commissioner shall be appointed for a period of 3 years, and may from time to time be reappointed.

(4) The Commissioner shall be entitled to such remuneration and allowances as are determined by the Chief Executive.

(5) The Chief Executive may, on the recommendation of the Chief Justice, revoke the appointment of the Commissioner for good cause.

(6) In this section, "eligible judge" (合資格法官) means –

(*a*) a Justice of Appeal of the Court of Appeal;

(*b*) a judge of the Court of First Instance;

(*c*) a former permanent judge of the Court of Final Appeal;

(*d*) a former Justice of Appeal of the Court of Appeal; or

(*e*) a former judge of the Court of First Instance.

39. Functions of Commissioner

The functions of the Commissioner are –

(*a*) to oversee the compliance by departments and their officers with the relevant requirements; and

(*b*) without limiting the generality of paragraph (*a*), to –

(i) conduct reviews under Division 2;

(ii) carry out examinations under Division 3;

(iii) submit reports to the Chief Executive and make recommendations to the Secretary for Security and heads of departments under Division 4;

(iv) perform any further functions prescribed by regulation made under section 62 for the purposes of this subparagraph; and

(v) perform such other functions as are imposed or conferred on him under this Ordinance or any other enactment.

Division 2 – Reviews by Commissioner

40. Reviews on compliance with relevant requirements

(1) The Commissioner shall conduct such reviews as he considers necessary on compliance by departments and their officers with the relevant requirements.

(2) Upon the conduct of any review under subsection (1), the Commissioner shall record in writing –

(*a*) details, as identified in the review, of any case of failure by any department or any of its officers to comply with any relevant requirement; and

(*b*) any other finding he has made in the review.

41. Notifications to departments concerned, etc.

(1) The Commissioner shall notify the head of any department concerned of his findings in a review under section 40(2).

(2) On being notified of the findings of the Commissioner under subsection (1), the head of the department shall submit to the Commissioner a report with details of any measures taken by the department to address any issues identified in the findings, as soon as reasonably practicable after the notification or, where the Commissioner has specified any period for submission of the report when giving the notification, within that period.

(3) Without prejudice to sections 47 and 48, the Commissioner may, whether before or after the head of the department has submitted a report to him under subsection (2), refer the findings and any other matters he thinks fit to the Chief Executive or the Secretary for Justice or both.

Division 3 – Examinations by Commissioner

42. Application for examination

(1) A person may apply to the Commissioner for an examination under this Division, if he believes –

(*a*) that any communication transmitted to or by him has been intercepted by a department; or

(*b*) that he is the subject of any covert surveillance that has been carried out by a department.

(2) The application is to be made in writing.

43. Examination by Commissioner

(1) Where the Commissioner receives an application under section 42, he shall, subject to section 44, 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 a prescribed authorization should have been, but has not been, issued or renewed under this Ordinance in relation to the interception or covert surveillance alleged.

(2) If, on an examination, the Commissioner determines that a prescribed authorization should have been, but has not been, issued or renewed under this Ordinance in relation to the interception or covert surveillance alleged, he –

(*a*) shall give notice to the applicant stating that he has found the case in the applicant's favour; and

(*b*) may, if he thinks fit, make an order for the payment of compensation by the Government to the applicant.

(3) If, on an examination, the Commissioner makes a determination other than that referred to in subsection (2), he shall give notice to the applicant stating that he has not found the case in the applicant's favour.

(4) The compensation ordered to be paid under subsection (2)(*b*) may include compensation for injury to feelings.

(5) Notwithstanding subsections (2) and (3), the Commissioner shall not give any notice or make any order under those subsections for so long as he considers that the giving of the notice or the making of the order (as the case may be) would be prejudicial to the prevention or detection of crime or the protection of public security.

44. Grounds for not carrying out examination, etc.

(1) Where, before or in the course of an examination, the Commissioner considers –

(*a*) that the application for the examination is received by the Commissioner more than 1 year after the day on which the interception or covert surveillance is alleged to have taken place or, where the interception or covert surveillance is alleged to have taken place on more than 1 day, the last occasion on which it is alleged to have taken place, and that it is not unfair for him not to carry out the examination;

(*b*) that the application is made anonymously;

(*c*) that the applicant cannot be identified or traced; or

(*d*) that, having regard to all the circumstances of the case, the application is frivolous or vexatious or is not made in good faith,

the Commissioner may refuse to carry out the examination or, where the examination has been commenced, to proceed with the carrying out of the examination (including the making of any determination further to the examination).

(2) Where, before or in the course of an examination, the Commissioner is satisfied that any relevant criminal proceedings are pending or

are likely to be instituted, the Commissioner shall not carry out the examination or, where the examination has been commenced, proceed with the carrying out of the examination (including the making of any determination further to the examination) –

(*a*) in the case of any pending criminal proceedings, until they have been finally determined or finally disposed of; or

(*b*) in the case of any criminal proceedings which are likely to be instituted, until they have been finally determined or finally disposed of or, if applicable, until they are no longer likely to be instituted.

(3) For the purposes of subsection (2), criminal proceedings are, in relation to an examination, regarded as relevant if, but only if, the interception or covert surveillance alleged in the application for the examination is or may be relevant to the determination of any question concerning any evidence which has been or may be adduced in those proceedings.

45. Further provisions relating to examinations

(1) For the purposes of an examination, the Commissioner shall –

(*a*) except as otherwise provided in this Ordinance, apply the principles applicable by a court on an application for judicial review; and

(*b*) carry out the examination on the basis of written submissions made to him.

(2) Without prejudice to section 51(3), for the purposes of an examination, the applicant is not entitled to have access to any information, document or other matter compiled by, or made available to, the Commissioner in connection with the examination.

(3) Without prejudice to section 43(5), in giving notice to an applicant under section 43(2)(*a*) or (3), the Commissioner shall not –

(*a*) give reasons for his determination;

(*b*) give details of any interception or covert surveillance concerned; and

(*c*) in the case of section 43(3), indicate whether or not the interception or covert surveillance alleged has taken place.

46. Notifications to departments concerned, etc.

(1) Where, on an examination, the Commissioner makes a determination under section 43(2), he shall notify the head of the department concerned of the determination.

(2) On being notified of the determination under subsection (1), the head of the department shall submit to the Commissioner a report with details of any measures taken by the department to address any issues arising from the determination, as soon as reasonably practicable after the notification or, where the Commissioner has specified any period for submission of the report when giving the notification, within that period.

(3) Without prejudice to sections 47 and 48, the Commissioner may, whether before or after the head of the department has submitted a report to him under subsection (2), refer the determination and any other matters he thinks fit to the Chief Executive or the Secretary for Justice or both.

Division 4 – Reports and Recommendations by Commissioner

47. Annual reports to Chief Executive by Commissioner

(1) The Commissioner shall, for each report period, submit a report to the Chief Executive.

(2) A report for a report period is to set out, separately in relation to interception and covert surveillance –

(*a*) a list showing –

(i) the number of prescribed authorizations issued under this Ordinance during the report period, and

the average duration of the prescribed authorizations;

(ii) the number of prescribed authorizations renewed under this Ordinance during the report period, and the average duration of the renewals;

(iii) the number of applications for the issue of prescribed authorizations made under this Ordinance that have been refused during the report period; and

(iv) the number of applications for the renewal of prescribed authorizations made under this Ordinance that have been refused during the report period;

(*b*) a list showing –

(i) the major categories of offences for the investigation of which prescribed authorizations have been issued or renewed under this Ordinance during the report period; and

(ii) the number of persons arrested during the report period as a result of or further to any interception or covert surveillance carried out pursuant to a prescribed authorization;

(*c*) a list showing –

(i) the number of device retrieval warrants issued under this Ordinance during the report period, and the average duration of the warrants; and

(ii) the number of applications for the issue of device retrieval warrants made under this Ordinance that have been refused during the report period;

(*d*) a list showing –

(i) a summary of reviews conducted by the Commissioner under section 40 during the report period;

(ii) the number and broad nature of any cases of irregularities identified in the reviews during the report period;

(iii) the number of applications for examination that have been received by the Commissioner during the report period;

(iv) a summary of the determinations of the Commissioner on examinations carried out during the report period; and

(v) the broad nature of recommendations made by the Commissioner under sections 49 and 50 during the report period; and

(*e*) an assessment on the overall compliance with the relevant requirements during the report period.

(3) The report is to be submitted within 6 months after the expiry of the report period.

(4) Subject to subsection (5), the Chief Executive shall cause a copy of the report to be laid on the table of the Legislative Council.

(5) If the Chief Executive considers that the publication of any matter in the report referred to in subsection (4) would be prejudicial to the prevention or detection of crime or the protection of public security, he may, after consultation with the Commissioner, exclude such matter from the copy of the report to be laid on the table of the Legislative Council under that subsection.

(6) In this section, "report period" (報告期間), in relation to a report required to be submitted under subsection (1), means –

(*a*) the period beginning on the commencement of this Ordinance and ending on 31 December in the same year; or

(*b*) any of the succeeding periods of 12 months ending on 31 December.

48. Other reports to Chief Executive by Commissioner

In addition to any report required to be submitted to the Chief Executive under section 47, the Commissioner may from time to time submit any further report to the Chief Executive on any matter relating to the performance of his functions under this Ordinance as he thinks fit.

49. Recommendations to Secretary for Security on code of practice

(1) If, in the course of performing any of his functions under this Ordinance, the Commissioner considers that any provision of the code of practice should be revised to better carry out the objects of this Ordinance, he may make such recommendations to the Secretary for Security as he thinks fit.

(2) Where the Commissioner makes any recommendations to the Secretary for Security under subsection (1), the Secretary shall notify the Commissioner of any exercise of power by him under section 59(3) to implement the recommendations, as soon as reasonably practicable after the recommendations have been made or, where the Commissioner has specified any period for the issue of the notification when making the recommendations, within that period.

50. Recommendations to departments

(1) If, in the course of performing any of his functions under this Ordinance, the Commissioner considers that any arrangements made by any department should be changed to better carry out the objects of this Ordinance or

the provisions of the code of practice, he may make such recommendations to the head of the department as he thinks fit.

(2) Where the Commissioner makes any recommendations to the head of the department under subsection (1), the head of the department shall submit to the Commissioner a report with details of any measures taken by the department to implement the recommendations, as soon as reasonably practicable after the recommendations have been made or, where the Commissioner has specified any period for submission of the report when making the recommendations, within that period.

(3) Without prejudice to sections 47 and 48, the Commissioner may, whether before or after the head of the department has submitted a report to him under subsection (2), refer the recommendations and any other matters he thinks fit to the Chief Executive or the Secretary for Justice or both.

Division 5 – Further Provisions Relating to Performance of Functions by Commissioner

51. Further powers of Commissioner

(1) For the purpose of performing any of his functions under this Ordinance, the Commissioner may –

(*a*) require any public officer or any other person to answer any question, and to provide any information, document or other matter in his possession or control to the Commissioner, within the time and in the manner specified by the Commissioner when making the requirement; and

(*b*) require any officer of a department to prepare any report on any case of interception or covert surveillance handled by the department, or on any class of such cases, within the time and in the manner specified by the Commissioner when making the requirement.

(2) Notwithstanding any other provision of this Ordinance or any other law, any person on whom a requirement is imposed by the Commissioner under subsection (1) shall comply with the requirement.

(3) Except as otherwise provided in this Ordinance, the Commissioner shall not be required to produce in any court or to divulge or communicate to any court, or to provide or disclose to any person, any information, document or other matter compiled by, or made available to, him in the course of performing any of his functions under this Ordinance.

(4) Except as otherwise provided in this Ordinance, the Commissioner may determine the procedure to be adopted in performing any of his functions under this Ordinance.

52. General obligations of departments to report on non-compliance

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.

53. Commissioner not regarded as court

In performing any of his functions under this Ordinance, the Commissioner is for all purposes not regarded as a court or a member of a court.

PART 5

FURTHER SAFEGUARDS

54. Regular reviews

(1) The head of each department shall make arrangements to keep under regular review the compliance by officers of the department with the relevant requirements.

(2) Without prejudice to subsection (1), where the head of any department has made any designation under section 7, he shall make arrangements for officers of a rank higher than those held by the authorizing officers of the department to keep under regular review the performance by the authorizing officers of any function under this Ordinance.

55. Discontinuance of interception or covert surveillance

(1) If, in the course of or further to any regular review conducted under section 54(1) or (2), the officer by whom the regular review is or has been conducted is of the opinion that any ground for discontinuance of a prescribed authorization exists, he shall, as soon as reasonably practicable after forming the opinion, cause the interception or covert surveillance concerned to be discontinued.

(2) Without prejudice to subsection (1), where a prescribed authorization has been issued or renewed under this Ordinance, the officer of the department concerned who is for the time being in charge of the interception or covert surveillance concerned –

(*a*) shall, as soon as reasonably practicable after he becomes aware that any ground for discontinuance of the prescribed authorization exists, cause the interception or covert surveillance to be discontinued; and

(*b*) may at any time cause the interception or covert surveillance to be discontinued.

(3) Where any officer has caused any interception or covert surveillance to be discontinued, whether under subsection (1) or (2), he shall, as soon as reasonably practicable after the discontinuance, cause a report on the discontinuance and the ground for the discontinuance to be provided to the relevant authority to whom an application under this Ordinance for the issue or renewal of the prescribed authorization concerned has last been made.

(4) Where the relevant authority receives a report under subsection (3), he shall, as soon as reasonably practicable after receiving the report, revoke the prescribed authorization concerned.

(5) Where any prescribed authorization is revoked under subsection (4), the prescribed authorization is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.

(6) For the purposes of this section, a ground for discontinuance of a prescribed authorization exists if –

(*a*) the conditions for the continuance of the prescribed authorization under section 3 are not met; or

(*b*) the relevant purpose of the prescribed authorization has been achieved.

(7) In this section, "relevant duration provision" (有關時限條文) means section 10(*b*), 13(*b*), 16(*b*), 19(*b*) or 22(1)(*b*) (as may be applicable).

56. Safeguards for protected products

(1) Where any protected product has been obtained pursuant to any prescribed authorization issued or renewed under this Ordinance on an application by any officer of a department, the head of the department shall make arrangements to ensure –

(*a*) that the following are limited to the minimum that is necessary for the relevant purpose of the prescribed authorization –

(i) the extent to which the protected product is disclosed;

(ii) the number of persons to whom any of the protected product is disclosed;

(iii) the extent to which the protected product is copied; and

(iv) the number of copies made of any of the protected product;

(*b*) that all practicable steps are taken to ensure that the protected product is protected against unauthorized or accidental access, processing, erasure or other use; and

(*c*) that the protected product is destroyed as soon as its retention is not necessary for the relevant purpose of the prescribed authorization.

(2) For the purposes of this section, something is necessary for the relevant purpose of a prescribed authorization if –

(*a*) it continues to be, or is likely to become, necessary for the relevant purpose; or

(*b*) except in the case of a prescribed authorization for a telecommunications interception, it is necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted.

57. Record keeping

(1) Without prejudice to section 56, each department shall keep a record which is to contain –

(*a*) in respect of each application for the issue or renewal of a prescribed authorization under this Ordinance by any officer of the department, a record of –

(i) the application (including a copy of any affidavit or statement provided under Part 3 for the purposes of the application); and

(ii) the determination in respect of the application by the relevant authority (including a copy of any prescribed authorization issued or renewed under Part 3 as a result of the application);

(*b*) in respect of each application for confirmation of an emergency authorization by any officer of the department as provided for in section 23(1), a record of –

(i) the application (including a copy of any affidavit provided under section 23(2)(*b*) or, where section 28 applies, a copy of any record, affidavit or other document provided as described in section 28(1)(*b*), for the purposes of the application); and

(ii) the determination in respect of the application by a panel judge (including a copy of any endorsement made or, where section 28 applies, a copy of any emergency authorization issued, under section 24(5) as a result of the application);

(*c*) in respect of each application for confirmation of a prescribed authorization or renewal by any officer of the department as provided for in section 26(1), a record of –

(i) the application (including a copy of any record, affidavit or statement provided under section 26(2)(*b*) for the purposes of the application); and

(ii) the determination in respect of the application by the relevant authority (including a copy of any prescribed authorization issued or renewed under section 27(5) as a result of the application);

(*d*) a record of –

(i) any case in which any interception or covert surveillance has been discontinued by any officer of the department under section 55; and

(ii) any case in which any prescribed authorization has been revoked under section 55 further to the discontinuance;

(*e*) in respect of each application for the issue of a device retrieval warrant under section 32 by any officer of the department, a record of –

(i) the application (including a copy of any affidavit provided under section 32(2)(*b*) for the purposes of the application); and

(ii) the determination in respect of the application by a panel judge (including a copy of any device retrieval warrant issued under section 33(3) as a result of the application);

(*f*) a record of –

(i) any case to which section 23(3) applies by reason that no application for confirmation of an emergency authorization is made within the period of 48 hours by any officer of the department;

(ii) any case to which section 26(3) applies by reason that no application for confirmation of a prescribed authorization or renewal is made within the period of 48 hours by any officer of the department; and

(iii) any findings in respect of any other irregularities and errors identified or detected by any officer of the department, whether in any regular review conducted under section 54(1) and (2) or otherwise; and

(*g*) any record reasonably required to be kept by the department to enable the Commissioner to prepare reports for submission to the Chief Executive under section 47, or

otherwise to perform any of his functions under this Ordinance.

(2) The record kept under subsection (1) –

(*a*) to the extent that it relates to any prescribed authorization or device retrieval warrant –

(i) is to be retained for a period of at least 2 years after the day on which the prescribed authorization or device retrieval warrant (as the case may be) has ceased to have effect; and

(ii) without prejudice to subparagraph (i), where it has come to the notice of the department concerned that any relevant civil or criminal proceedings before any court are pending or are likely to be instituted, or any relevant review is being conducted under section 40, or, in the case of a prescribed authorization, any relevant application for an examination has been made under section 42, is to be retained –

(A) in the case of any pending proceedings, review or application, at least until the pending proceedings or application has been finally determined or finally disposed of or until the review has been completed or finally disposed of (as the case may be); or

(B) in the case of any proceedings which are likely to be instituted, at least until they have been finally determined or finally disposed of or, if applicable, until they are no longer likely to be instituted; or

(*b*) to the extent that it does not relate to any prescribed authorization or device retrieval warrant, is to be retained for a period of at least 2 years.

(3) For the purposes of subsection (2), any proceedings, review or application is, in relation to any part of a record that relates to any prescribed authorization or device retrieval warrant, regarded as relevant if, but only if –

(*a*) the prescribed authorization or device retrieval warrant (as the case may be) is or may be relevant to the determination of any question for the purposes of the proceedings, review or application (as the case may be); or

(*b*) in the case of a prescribed authorization, any protected product obtained pursuant to the prescribed authorization is or may be relevant to the determination of any question for the purposes of the proceedings, review or application (as the case may be).

58. Non-admissibility of telecommunications interception product

(1) Any telecommunications interception product shall not be admissible in evidence in any proceedings before any court other than to prove that a relevant offence has been committed.

(2) Any telecommunications interception product, and any particulars as to a telecommunications interception carried out pursuant to a relevant prescribed authorization, shall not be made available to any party to any proceedings before any court (other than any such proceedings instituted for a relevant offence).

(3) In any proceedings before any court (other than any such proceedings instituted for a relevant offence), any evidence or question which tends to suggest any of the following matters shall not be adduced or asked –

(*a*) that an application has been made for the issue or renewal of a relevant prescribed authorization, or the issue of a relevant device retrieval warrant, under this Ordinance;

(*b*) that a relevant prescribed authorization has been issued or renewed, or a relevant device retrieval warrant has been issued, under this Ordinance;

(*c*) that any requirement has been imposed on any person to provide assistance for the execution of a relevant prescribed authorization or a relevant device retrieval warrant;

(*d*) that any information has been obtained pursuant to a relevant prescribed authorization.

(4) This section is not to be construed as prohibiting the disclosure of any information that continues to be available for disclosure, to the extent that –

(*a*) the disclosure is made to ensure that a person conducting the prosecution of any offence has the information he needs to determine what is required of him by his duty to secure the fairness of the trial of that offence; or

(*b*) the disclosure is made to a judge alone in a case in which the judge has ordered the disclosure to be so made to him.

(5) A judge may only order a disclosure under subsection (4)(*b*) if he is satisfied that the disclosure is essential in the interests of justice.

(6) Where a judge orders a disclosure under subsection (4)(*b*), and in consequence of that disclosure he considers that it is essential in the interests of justice, he may direct the person conducting the prosecution of any offence to make for the purposes of the proceedings concerned any such admission of fact as the judge considers essential to secure the fairness of the trial of that offence.

(7) Notwithstanding subsection (6), no direction made under that subsection authorizes or requires anything to be done in contravention of subsections (1), (2) and (3).

(8) In this section –

"party" (一方), in relation to any criminal proceedings, includes the prosecution;

"relevant device retrieval warrant" (有關器材取出手令) means a device retrieval warrant for the retrieval of any of the devices authorized to be used under a relevant prescribed authorization;

"relevant offence" (有關罪行) means any offence constituted by the disclosure of any telecommunications interception product or of any information relating to the obtaining of any telecommunications interception product (whether or not there are other constituent elements of the offence);

"relevant prescribed authorization" (有關訂明授權) means a prescribed authorization for a telecommunications interception;

"telecommunications interception product" (電訊截取成果) means any interception product to the extent that it is –

(*a*) any contents of a communication that have been obtained pursuant to a relevant prescribed authorization; or

(*b*) a copy of such contents.

59. Code of practice

(1) The Secretary for Security shall issue a code of practice for the purpose of providing practical guidance to officers of the departments in respect of matters provided for in this Ordinance.

(2) Without limiting the generality of subsection (1), the Secretary for Security may in the code of practice specify the form of any application to be made to a panel judge under this Ordinance.

(3) The Secretary for Security may from time to time revise the whole or any part of the code of practice, in a manner consistent with his power to issue the code under this section, and, unless the context otherwise requires, any reference to the code of practice, whether in this Ordinance or otherwise, is to be construed as a reference to the code as so revised.

(4) Any officer of a department shall, in performing any function under or for the purposes of any provision of this Ordinance, have regard to the provisions of the code of practice.

(5) A failure on the part of any person to comply with any provision of the code of practice –

(*a*) is for all purposes not of itself to be regarded as a failure to comply with any provision of this Ordinance; and

(*b*) without prejudice to paragraph (*a*), does not affect the validity of any prescribed authorization or device retrieval warrant.

PART 6

MISCELLANEOUS

60. Prescribed authorizations and device retrieval warrants not affected by minor defects

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

(2) Without prejudice to the generality of subsection (1), any information (including any protected product) obtained pursuant to a prescribed authorization is not by reason only of any minor defect in the prescribed authorization to be rendered inadmissible in evidence in any proceedings before any court.

(3) For the purposes of this section, any reference to minor defect, in relation to a prescribed authorization or device retrieval warrant, includes any defect or irregularity, other than a substantial defect or irregularity, in or in connection with –

(*a*) the issue, or the purported issue, of that prescribed authorization or device retrieval warrant or of a document

purporting to be that prescribed authorization or device retrieval warrant; or

(*b*) the execution, or the purported execution, of that prescribed authorization or device retrieval warrant or of a document purporting to be that prescribed authorization or device retrieval warrant.

61. Immunity

(1) Subject to subsection (2), a person shall not incur any civil or criminal liability by reason only of –

(*a*) any conduct carried out pursuant to a prescribed authorization or device retrieval warrant (including any conduct incidental to such conduct);

(*b*) his performance or purported performance in good faith of any function under this Ordinance; or

(*c*) his compliance with a requirement made or purportedly made under this Ordinance.

(2) Nothing in subsection (1) affects any liability that is or may be incurred by any person by reason only of –

(*a*) any entry onto any premises without permission; or

(*b*) any interference with any property without permission.

62. Regulation

The Chief Executive in Council may make regulation for –

(*a*) the better carrying out of the purposes of this Ordinance; and

(*b*) without limiting the generality of paragraph (*a*), prescribing any matter which this Ordinance provides is, or may be, prescribed by regulation made under this section.

63. Amendment of Schedules

The Chief Executive in Council may, by notice published in the Gazette, amend Schedules 1, 2, 3 and 4.

64. Repeal and consequential amendments

(1) The Interception of Communications Ordinance (Cap. 532) is repealed.

(2) The enactments specified in Schedule 5 are amended as set out in that Schedule.

65. Transitional arrangements

(1) Where any materials have been obtained by or on behalf of any department by carrying out any telecommunications interception pursuant to an order issued or renewed before the commencement of this Ordinance under the provision then in force as section 33 of the Telecommunications Ordinance (Cap. 106), sections 56 and 58 apply, with necessary modifications, to the materials, to the extent that they are any of the contents of the communication intercepted or a copy of such contents, and to the relevant matters as if –

(*a*) the order were a prescribed authorization issued or renewed under this Ordinance, and accordingly –

(i) the materials were, for the purposes of sections 56 and 58 respectively, protected product and telecommunications interception product; and

(ii) the application for the issue or renewal of the order were an application for the issue or renewal of a prescribed authorization under this Ordinance; and

(*b*) the purpose sought to be furthered by carrying out the operation required to be carried out under the order were the relevant purpose of the order.

(2) Subsection (1) is in addition to and not in derogation of section 23 of the Interpretation and General Clauses Ordinance (Cap. 1).

(3) In this section –

"copy" (文本), in relation to any contents of a communication referred to in subsection (1), means any of the following (whether or not in documentary form) –

(*a*) any copy, extract or summary of such contents which identifies itself as such copy, extract or summary of such contents;

(*b*) any record referring to the interception referred to in subsection (1) which is a record of the identity of any person who is the sender or intended recipient of the communication;

"relevant matters" (有關事宜) –

(*a*) in relation to section 58(2), means any particulars as to the telecommunications interception referred to in subsection (1); and

(*b*) in relation to section 58(3), means any evidence or question which tends to suggest any of the following matters –

(i) that an application has been made for the issue or renewal of the order referred to in subsection (1);

(ii) that the order has been issued or renewed;

(iii) that any requirement has been imposed on any person to provide assistance for the execution of the order;

(iv) that any information has been obtained pursuant to the order.

SCHEDULE 1 [ss. 2 & 63]

DEPARTMENTS

PART 1

DEPARTMENTS SPECIFIED FOR INTERCEPTION, ETC.

1. Customs and Excise Department
2. Hong Kong Police Force
3. Independent Commission Against Corruption

PART 2

DEPARTMENTS SPECIFIED FOR COVERT SURVEILLANCE, ETC.

1. Customs and Excise Department
2. Hong Kong Police Force
3. Immigration Department
4. Independent Commission Against Corruption

SCHEDULE 2 [ss. 2, 6 & 63]

PROCEDURES OF, AND OTHER MATTERS RELATING TO, PANEL JUDGE

1. **Provisions for consideration of applications by panel judge**

(1) A panel judge shall consider any application made to him under this Ordinance in private.

(2) Without prejudice to subsection (1), the application may, where the panel judge so directs, be considered at any place other than within the court precincts.

(3) Without prejudice to Division 5 of Part 3 of this Ordinance, nothing in this section prevents consideration of the application by the panel judge on the basis of written submissions made to him.

2. **Further powers of panel judge**

For the purpose of performing any of his functions under this Ordinance, a panel judge may administer oaths and take affidavits.

3. **Provisions for documents and records compiled by or made available to panel judge**

(1) A panel judge shall cause all documents and records compiled by, or made available to, him for any purpose related to the performance of any of his functions under this Ordinance to be kept in a packet sealed by his order, as soon as they are no longer immediately required for the purpose of performing any of his functions under this Ordinance.

(2) Notwithstanding subsection (1), a panel judge to whom any documents or records are made available in the circumstances described in that subsection shall –

(*a*) cause a copy of each of the documents or records so made available to him to be certified by affixing his seal to it and signing on it; and

(*b*) cause the copy so certified to be made available to the department concerned.

(3) Where any documents or records are kept in a packet under subsection (1) –

(*a*) the packet is to be kept in a secure place specified by a panel judge;

(*b*) the packet may not be opened, and the documents or records may not be removed from the packet, except pursuant to an order of a panel judge made for the purpose

of performing any of his functions under this Ordinance; and

(*c*) the packet, and the documents or records, may not be destroyed except pursuant to an order of a panel judge.

(4) Where any packet is opened pursuant to any order of a panel judge referred to in subsection (3)(*b*) –

(*a*) if any documents or records have been removed from the packet, the panel judge shall cause the documents or records to be returned to be kept in the packet, as soon as they are no longer immediately required for the purpose of performing any of his functions under this Ordinance; and

(*b*) the panel judge shall cause the packet to be sealed by his order, as soon as access to the documents or records kept in it is no longer immediately required for the purpose of performing any of his functions under this Ordinance,

and the provisions of subsection (3) apply, with necessary modifications, to the packet so sealed as they apply to the packet referred to in subsection (1).

(5) Nothing in this section prevents any of the documents and records referred to in subsection (1), or any copies of such documents and records, to be made available to the department concerned for the purposes of any relevant written determination provision or otherwise pursuant to an order of a panel judge.

(6) In this section, "relevant written determination provision" (有關書面決定條文) means section 9(3), 12(3), 24(5) (whether with or without reference to section 28 of this Ordinance), 27(5) or 33(3) of this Ordinance.

4. **Panel judge to act judicially but not regarded as court**

In performing any of his functions under this Ordinance, a panel judge shall act judicially and have the same powers, protection and immunities as a

judge of the Court of First Instance has in relation to proceedings in that Court, although he is for all purposes not regarded as a court or a member of a court.

SCHEDULE 3 [ss. 8, 11, 14, 17, 20 & 63]

REQUIREMENTS FOR AFFIDAVIT OR STATEMENT FOR APPLICATION FOR ISSUE OR RENEWAL OF PRESCRIBED AUTHORIZATION FOR INTERCEPTION OR COVERT SURVEILLANCE

PART 1

APPLICATION FOR ISSUE OF JUDICIAL AUTHORIZATION FOR INTERCEPTION

An affidavit supporting an application for the issue of a judicial authorization for interception is to –

(*a*) state which of the purposes specified in section 3(1)(*a*)(i) and (ii) of this Ordinance is sought to be furthered by carrying out the interception;

(*b*) set out –

(i) the form of the interception and the information sought to be obtained by carrying out the interception;

(ii) if known, the identity of any person who is to be the subject of the interception;

(iii) if known, particulars of the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying any communication that is to be intercepted;

(iv) the proposed duration of the interception;

(v) the nature of, and an assessment of the immediacy and gravity of –

(A) where the purpose sought to be furthered by carrying out the interception is that specified in section 3(1)(*a*)(i) of this Ordinance, the serious crime to be prevented or detected; or

(B) where the purpose sought to be furthered by carrying out the interception is that specified in section 3(1)(*a*)(ii) of this Ordinance, the particular threat to public security;

(vi) the benefits likely to be obtained by carrying out the interception;

(vii) an assessment of the impact (if any) of the interception on any person other than that referred to in subparagraph (ii);

(viii) the likelihood that any information which may be subject to legal professional privilege will be obtained by carrying out the interception; and

(ix) the reason why the purpose sought to be furthered by carrying out the interception cannot reasonably be furthered by other less intrusive means; and

(*c*) identify by name and rank the applicant.

PART 2

APPLICATION FOR ISSUE OF JUDICIAL AUTHORIZATION FOR TYPE 1 SURVEILLANCE

An affidavit supporting an application for the issue of a judicial authorization for Type 1 surveillance is to –

(*a*) state which of the purposes specified in section 3(1)(*a*)(i) and (ii) of this Ordinance is sought to be furthered by carrying out the Type 1 surveillance;

(*b*) set out –

(i) the form of the Type 1 surveillance (including the kind or kinds of any devices to be used) and the information sought to be obtained by carrying out the Type 1 surveillance;

(ii) if known, the identity of any person who is to be the subject of the Type 1 surveillance;

(iii) the identity of any person, other than that referred to in subparagraph (ii), who may be affected by the Type 1 surveillance or, if the identity of such person is not known, the description of any such person or class of such persons who may be affected by the Type 1 surveillance;

(iv) if known, particulars of any premises or any object or class of objects in or on which the Type 1 surveillance is to be carried out;

(v) the proposed duration of the Type 1 surveillance;

(vi) the nature of, and an assessment of the immediacy and gravity of –

(A) where the purpose sought to be furthered by carrying out the Type 1 surveillance is

that specified in section 3(1)(*a*)(i) of this Ordinance, the serious crime to be prevented or detected; or

(B) where the purpose sought to be furthered by carrying out the Type 1 surveillance is that specified in section 3(1)(*a*)(ii) of this Ordinance, the particular threat to public security;

(vii) the benefits likely to be obtained by carrying out the Type 1 surveillance;

(viii) an assessment of the impact (if any) of the Type 1 surveillance on any person referred to in subparagraph (iii);

(ix) the likelihood that any information which may be subject to legal professional privilege will be obtained by carrying out the Type 1 surveillance; and

(x) the reason why the purpose sought to be furthered by carrying out the Type 1 surveillance cannot reasonably be furthered by other less intrusive means; and

(*c*) identify by name and rank the applicant.

PART 3

APPLICATION FOR ISSUE OF EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE

A statement supporting an application for the issue of an executive authorization for Type 2 surveillance is to –

(*a*) state which of the purposes specified in section 3(1)(*a*)(i) and (ii) of this Ordinance is sought to be furthered by carrying out the Type 2 surveillance;

(*b*) set out –

(i) the form of the Type 2 surveillance (including the kind or kinds of any devices to be used) and the information sought to be obtained by carrying out the Type 2 surveillance;

(ii) if known, the identity of any person who is to be the subject of the Type 2 surveillance;

(iii) the identity of any person, other than that referred to in subparagraph (ii), who may be affected by the Type 2 surveillance or, if the identity of such person is not known, the description of any such person or class of such persons who may be affected by the Type 2 surveillance;

(iv) if known, particulars of any premises or any object or class of objects in or on which the Type 2 surveillance is to be carried out;

(v) the proposed duration of the Type 2 surveillance;

(vi) the nature of, and an assessment of the immediacy and gravity of –

(A) where the purpose sought to be furthered by carrying out the Type 2 surveillance is that specified in section 3(1)(*a*)(i) of this Ordinance, the serious crime to be prevented or detected; or

(B) where the purpose sought to be furthered by carrying out the Type 2 surveillance is that specified in section 3(1)(*a*)(ii) of this

Ordinance, the particular threat to public security;

(vii) the benefits likely to be obtained by carrying out the Type 2 surveillance;

(viii) an assessment of the impact (if any) of the Type 2 surveillance on any person referred to in subparagraph (iii);

(ix) the likelihood that any information which may be subject to legal professional privilege will be obtained by carrying out the Type 2 surveillance; and

(x) the reason why the purpose sought to be furthered by carrying out the Type 2 surveillance cannot reasonably be furthered by other less intrusive means; and

(*c*) identify by name and rank the applicant.

PART 4

APPLICATION FOR RENEWAL OF JUDICIAL AUTHORIZATION OR EXECUTIVE AUTHORIZATION FOR INTERCEPTION OR COVERT SURVEILLANCE

An affidavit or statement supporting an application for the renewal of a judicial authorization for interception or Type 1 surveillance or an executive authorization for Type 2 surveillance is to –

(*a*) set out –

(i) whether the renewal sought is the first renewal and, if not, each occasion on which the judicial authorization or executive authorization has been renewed previously;

(ii) any significant change to any information previously provided in any affidavit or statement under this Ordinance for the purposes of any application for the issue or renewal of the judicial authorization or executive authorization, or for the purposes of any application made further to an oral application for confirmation of the judicial authorization or executive authorization or its previous renewal;

(iii) the value of the information so far obtained pursuant to the judicial authorization or executive authorization;

(iv) the reason why it is necessary to apply for the renewal; and

(v) the proposed duration of the interception, Type 1 surveillance or Type 2 surveillance (as the case may be); and

(*b*) identify by name and rank the applicant.

SCHEDULE 4 [ss. 32 & 63]

REQUIREMENTS FOR AFFIDAVIT FOR APPLICATION FOR ISSUE OF DEVICE RETRIEVAL WARRANT

An affidavit supporting an application for the issue of a device retrieval warrant for the retrieval of any of the devices authorized to be used under a prescribed authorization is to –

(*a*) set out –

(i) the kind or kinds of the devices sought to be retrieved;

(ii) particulars of the premises or object from which the devices are to be retrieved, and the reason why the applicant considers that the devices are in or on such premises or object;

(iii) the estimated time required to complete the retrieval;

(iv) an assessment of the impact (if any) of the retrieval on any person; and

(v) the need for the retrieval; and

(*b*) identify by name and rank the applicant.

SCHEDULE 5 [s. 64]

CONSEQUENTIAL AMENDMENTS

Post Office Ordinance

1. **Warrant of Chief Secretary for Administration for opening and delaying postal packets**

Section 13 of the Post Office Ordinance (Cap. 98) is repealed.

2. **Disposal of postal packets opened under section 10, 12 or 13**

(1) Section 14 is amended, in the heading, by repealing "**, 12 or 13**" and substituting "**or 12**".

(2) Section 14 is amended by repealing ", 12 or 13" and substituting "or 12".

3. **Extension of sections 12, 13 and 14 to articles not transmissible by post**

(1) Section 15 is amended, in the heading, by repealing "**, 13**".

(2) Section 15 is amended by repealing ", 13".

Post Office Regulations

4. **Regulation amended**

Regulation 10 of the Post Office Regulations (Cap. 98 sub. leg. A) is amended by repealing ", 12, or 13" and substituting "or 12".

Telecommunications Ordinance

5. **Section substituted**

Section 33 of the Telecommunications Ordinance (Cap. 106) is repealed and the following substituted –

"**33. Orders for interception of messages for provision of facilities**

(1) For the purpose of providing or making available facilities reasonably required for –

(*a*) the detection or discovery of any telecommunications service provided in contravention of any provision of this Ordinance or any regulation made under this Ordinance or any of the terms or conditions of a licence granted under this Ordinance; or

(*b*) the execution of prescribed authorizations for telecommunications interception that may from time to time be issued or renewed under the Interception of Communications and Surveillance Ordinance (of 2006),

the Chief Executive may order that any class of messages shall be intercepted.

(2) An order under subsection (1) shall not of itself authorize the obtaining of the contents of any individual message.

(3) In this section –

"contents" (內容), in relation to any message, has the meaning assigned to it in section 2(5) of the Interception of Communications and Surveillance Ordinance (of 2006) in relation to a communication referred to in that section;

"prescribed authorization" (訂明授權) has the meaning assigned to it in section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

"telecommunications interception" (電訊截取) has the meaning assigned to it in section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006).".

Prevention of Bribery Ordinance

6. **Public bodies**

Schedule 1 to the Prevention of Bribery Ordinance (Cap. 201) is amended by adding –

"107. Commissioner on Interception of Communications and Surveillance.".

Personal Data (Privacy) Ordinance

7. **Section added**

The Personal Data (Privacy) Ordinance (Cap. 486) is amended by adding –

"**58A. Protected product and relevant records under Interception of Communications and Surveillance Ordinance**

(1) A personal data system is exempt from the provisions of this Ordinance to the extent that it is used by a data user for the collection, holding, processing or use of personal data which are, or are contained in, protected product or relevant records.

(2) Personal data which are, or are contained in, protected product or relevant records are exempt from the provisions of this Ordinance.

(3) In this section –

"device retrieval warrant" (器材取出手令) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

"prescribed authorization" (訂明授權) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

"protected product" (受保護成果) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

"relevant records" (有關紀錄) means documents and records relating to –

(*a*) any application for the issue or renewal of any prescribed authorization or device retrieval warrant under the Interception of Communications and Surveillance Ordinance (of 2006); or

(*b*) any prescribed authorization or device retrieval warrant issued or renewed under that Ordinance (including anything done pursuant to or in relation to such prescribed authorization or device retrieval warrant).".

Official Secrets Ordinance

8. **Information related to commission of offences and criminal investigations**

Section 17(2)(*c*), (*d*) and (*e*) of the Official Secrets Ordinance (Cap. 521) is repealed and the following substituted –

"(*c*) any information, document or article which is interception product within the meaning of the Interception of Communications and Surveillance Ordinance (of 2006); or

(*d*) any information relating to the obtaining of any interception product described in paragraph (*c*).".

Explanatory Memorandum

The object of this Bill is to regulate the conduct of interception of communications and the use of surveillance devices by or on behalf of public officers.

2. The Bill contains 6 Parts and 5 Schedules.

Part 1 – Preliminary

3. Part 1 provides for preliminary matters –

(*a*) Clause 2 contains the definitions with reference to which the provisions of the Bill are to be interpreted. In particular –

(i) "interception" is defined to mean the carrying out of any intercepting act in respect of communications, and for that purpose –

- "communication" is defined to mean any communication transmitted by a postal service or by a telecommunications system; and
- "intercepting act" is defined to mean the inspection of any of the contents of a communication, in the course of its transmission, by persons other than its sender or its intended recipient;

(ii) "covert surveillance" is defined to mean systematic surveillance carried out with the use of any surveillance device for the purposes of a specific investigation or operation where, among other conditions that apply, any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy; and, for the purposes of the Bill, covert surveillance is further divided into "Type 1 surveillance" and "Type 2 surveillance" as defined under their respective definitions; and

(iii) "department" is defined, in relation to interception cases, to mean the Customs and Excise Department, the Hong Kong Police Force, and the Independent Commission Against Corruption, and, in relation to covert surveillance cases, to mean the same departments as well as the Immigration Department.

(*b*) Clause 3 sets out the conditions for the issue or renewal, or the continuance, of prescribed authorizations under the Bill. Under those conditions, any interception or covert surveillance sought to be authorized should be carried out for the purpose of preventing or detecting serious crime or for the purpose of protecting public security, and should, upon taking into consideration various specified matters, also be proportionate to such purpose.

<u>Part 2 – Prohibition on Interception and Covert Surveillance</u>

4. Part 2 contains the prohibition provisions –

(*a*) Clause 4 provides that no public officers shall, directly or through any other person, carry out any interception. This

prohibition does not apply if the interception is carried out pursuant to a prescribed authorization, or is carried out in respect of telecommunications transmitted by specified radiocommunications, or is otherwise authorized, permitted or required to be carried out under any other enactments.

(*b*) Clause 5 provides that no public officers shall, directly or through any other person, carry out any covert surveillance. This prohibition does not apply if the covert surveillance is carried out pursuant to a prescribed authorization.

Part 3 – Prescribed Authorizations, etc.

5. Part 3 contains provisions relating to prescribed authorization, and is divided into 6 Divisions –

(*a*) Division 1 (clauses 6 and 7) provides for the appointment and designation of panel judges and authorizing officers, being relevant authorities having functions to approve applications for the issue or renewal of prescribed authorizations, etc. under Part 3 –

(i) Clause 6 provides for the appointment of 3 to 6 eligible judges as panel judges by the Chief Executive on the recommendation of the Chief Justice. It also provides that Schedule 2 applies to the procedures and other matters relating to panel judges.

(ii) Clause 7 provides for the designation of officers not below a rank equivalent to that of senior superintendent of police as authorizing officers by the head of the departments.

(*b*) Division 2 (clauses 8 to 13) provides for the issue of judicial authorizations for interception or Type 1

surveillance, on the application to a panel judge by an officer of a department with the approval of a directorate officer of that department, and further for the renewal of judicial authorizations. Subject to the conditions set out in clause 3, a judicial authorization may be issued or renewed for a maximum term of 3 months.

(*c*) Division 3 (clauses 14 to 19) provides for the issue of executive authorizations for Type 2 surveillance, on the application to an authorizing officer of a department by an officer of that department, and further for the renewal of executive authorizations. Subject to the conditions set out in clause 3, an executive authorization may be issued or renewed for a maximum term of 3 months.

(*d*) Division 4 (clauses 20 to 24) provides for the issue of emergency authorizations for interception or Type 1 surveillance by the head of departments in any emergency cases where it is not practicable for judicial authorizations to be obtained from panel judges. However, while the conditions set out in clause 3 also apply to the issue of the emergency authorization, the emergency authorization is only to last for a maximum term of 48 hours and in any event is subject to confirmation on an application to a panel judge by an officer of the department concerned. Where the panel judge does not confirm the emergency authorization, he may order the revocation or variation of the emergency authorization, and may also order the destruction of any of the information obtained pursuant to the emergency authorization.

(*e*) Division 5 (clauses 25 to 28) provides for the alternative of making oral applications for the issue or renewal of

prescribed authorizations in specified circumstances, notwithstanding the requirements for written applications otherwise applicable to prescribed authorizations under Part 3. Where any oral application is made, supporting information may be provided orally, and the determination in respect of the application may also be delivered orally. However, the determination under an oral authorization is also subject to confirmation on an application to the relevant authority by whom the oral application has been determined. Where the relevant authority does not confirm the prescribed authorization or the renewal issued or granted under the determination, he may order the revocation or variation of the prescribed authorization or renewal, and may also order the destruction of any of the information obtained pursuant to the prescribed authorization or renewal.

(*f*) Division 6 (clauses 29 to 37) contains general provisions applicable to prescribed authorizations. Clauses 29 to 31 deal with matters that may be authorized, required or provided for by prescribed authorizations. Clauses 32 to 37 then provide for the issue, after a prescribed authorization has ceased to have effect, of a device retrieval warrant for the retrieval of devices previously installed in or on premises or objects pursuant to the prescribed authorization. The application is to be made to a panel judge by an officer of a department, and on considering the application, the panel judge may issue a device retrieval warrant for a maximum term of 3 months.

Part 4 – The Commissioner

6. Part 4 contains provisions relating to the Commissioner on Interception of Communications and Surveillance, and is divided into 5 Divisions –

(*a*) Division 1 (clauses 38 and 39) provides for the establishment of the office of the Commissioner and for his functions. The Commissioner is to be appointed by the Chief Executive on the recommendation of the Chief Justice. His functions are to oversee the compliance by departments and their officers with the relevant requirements (cf. definition of "relevant requirement" in clause 2), and in particular to perform functions set out in Divisions 2 to 4, and other functions prescribed by regulation made under clause 62 and generally by the Bill and by other enactments.

(*b*) Division 2 (clauses 40 and 41) provides for reviews conducted by the Commissioner on compliance by departments and their officers with the relevant requirements. The Commissioner is also to notify departments concerned of any case where he has made any findings that there has been failure by any department or any of its officers to comply with any relevant requirement.

(*c*) Division 3 (clauses 42 to 46) provides for examinations carried out by the Commissioner, on the application by any person who believes that he is the subject of any interception or covert surveillance carried out by a department. The Commissioner is to consider the case by adopting the judicial review principles and by reference to written submissions made to him. After consideration of the case, he is to notify the applicant whether he has found the case in the applicant's favour, and may, if he thinks fit,

make an order for the payment by the Government to the applicant of a sum of compensation, which may include compensation for injury to feelings. The Commissioner is also to notify the department concerned of any case where he has found the case in the applicant's favour.

(*d*) Division 4 (clauses 47 to 50) provides for the submission by the Commissioner to the Chief Executive of annual reports containing specified information, and then requires a copy of the reports to be laid on the table of the Legislative Council. The Commissioner may also from time to time make further reports to the Chief Executive, and may also make recommendations to the Secretary for Security and the departments on specified matters.

(*e*) Division 5 (clauses 51 to 53) contains further provisions relating to the performance of functions by the Commissioner. The Commissioner may impose requirements on public officers and other persons to provide information to him, and may require officers of departments to prepare reports in respect of cases of interception or covert surveillance handled by the departments. In addition, the head of a department is to keep the Commissioner informed of any case in which he considers that there may have been any case of failure by the department or any of its officers to comply with any relevant requirement.

Part 5 – Further Safeguards

7. Part 5 provides for further safeguards in respect of interception and covert surveillance carried out by departments –

(*a*) Under clauses 54 and 55, a department is to conduct regular reviews on the compliance by officers of the

department with the relevant requirements, and on the performance by authorizing officers of the department of any function under the Bill. Any interception or covert surveillance carried out pursuant to a prescribed authorization is to be discontinued once the officer by whom a regular review is conducted, or the officer in charge of the operation, considers that the conditions set out in clause 3 are not met, or that the relevant purpose of the prescribed authorization has been achieved (cf. definition of "relevant purpose" in clause 2). In addition, the officer in charge of the operation may at any time cause the operation to be discontinued. In any case where any operation is discontinued, the relevant authority by whom the prescribed authorization authorizing the operation has been issued or renewed is to be notified, and then to revoke the prescribed authorization.

(*b*) Under clause 56, each department shall make arrangements to ensure that any product obtained pursuant to a prescribed authorization (cf. definition of "protected product" in clause 2) is to be dealt with in accordance with specified arrangements, in order to minimize the extent to which the product is disclosed or copied, or subject to unauthorized or accidental access, processing, erasure or other use, and to ensure its timely destruction.

(*c*) Under clause 57, each department is also to keep a proper record in respect of specified matters, including matters relating to applications for the issue or renewal of prescribed authorizations or device retrieval warrants, and other matters provided for in the Bill. The record is, to the extent that it relates to any prescribed authorization or

device retrieval warrant, to be kept for a minimum term of 2 years after the prescribed authorization or device retrieval warrant ceases to have effect, and is in any event to be kept at least until any relevant pending or anticipated proceedings, etc. have been finally disposed of. The part of the record that relates to other matters is to be kept for a minimum term of 2 years.

(*d*) By virtue of clause 58, in any proceedings before any court (other than proceedings for specified offences (cf. definition of "relevant offence" in clause 58)), any product obtained pursuant to a prescribed authorization for interception of a communication transmitted by a telecommunications system (cf. definition of "telecommunications interception product" in clause 58) shall not be admissible in evidence and shall not be made available to any party, and any evidence or question which tends to suggest matters relating to any application for the issue or renewal of any relevant prescribed authorizations, and other related matters shall not be adduced or asked. However, the clause also provides that it does not prohibit disclosure in specified cases where the disclosure is required in the interests of justice, etc.

(*e*) Clause 59 further provides that the Secretary for Security is to issue a code of practice for the purpose of providing practical guidance to officers of the departments in respect of matters provided for in the Bill.

Part 6 - Miscellaneous

8. Part 6 contains miscellaneous provisions dealing with minor defects of prescribed authorizations and device retrieval warrants, immunity, regulation, and amendment of schedules. In addition, clause 64 seeks to repeal the

Interception of Communications Ordinance (Cap. 532) and to introduce consequential amendments to ordinances including the Post Office Ordinance (Cap. 98), the Telecommunications Ordinance (Cap. 106) and other appropriate ordinances. Further, clause 65 provides for a transitional arrangement so that, among other matters, any materials obtained by way of interception pursuant to an order issued or renewed under section 33 of the Telecommunications Ordinance (Cap. 106) before the commencement of the Bill as enacted are also subject to clauses 56 and 58 as if they were product obtained pursuant to a prescribed authorization.

Annex B

For information
7 February 2006

Legislative Council Panel on Security

Proposed Legislative Framework on Interception of Communications and Covert Surveillance

Purpose

This paper sets out proposals for new legislation regulating the conduct of interception of communications and covert surveillance by law enforcement agencies (LEAs).

Background

2. Interception of communications and covert surveillance are two related types of operations. Interception of communications is commonly understood as the interception of the content of telecommunications or postal articles in the course of their transmission by either telecommunications or postal service. Covert surveillance, on the other hand, commonly refers to systematic surveillance undertaken covertly, in situations where the person subject to surveillance is entitled to a reasonable expectation of privacy.

3. These covert investigation tools were a subject of discussions in society and in the former Legislative Council (LegCo) in the 1990's, arising from public concerns on their implications on privacy. In 1996, the Law Reform Commission (LRC) published a consultation paper on interception of communications and covert surveillance. Subsequently it published its report with recommendations for new legislation on interception of communications.

4. In response to the LRC report on **interception of communications**, the Administration published a Consultation Paper with a White Bill annexed in early 1997 incorporating many of the key recommendations of the LRC for consultation. In parallel, LegCo considered a private member's bill and enacted the Interception of Communications Ordinance (IOCO), whose commencement was withheld by the Chief Executive in Council in July 1997 due to its shortcomings. Since then the Administration has been conducting a comprehensive review on the subject of interception of communications. At the meeting of the LegCo Panel on Security on 10 June 2004, the Secretary for Security said that the Administration would strive to complete the review and revert to the Panel within the 2004-05 legislative

session. Developments since (please see paragraphs 5 and 6 below) have made it logical for us to consider the subject together with covert surveillance.

5. On **covert surveillance**, the LRC explained in 1996, when publishing its report on interception of communications, that it had focused on the issue of interception of communications first, and deferred the study of surveillance. It said that the Privacy Sub-committee of the LRC would continue to discuss the issue of surveillance after publication of the report on interception of communications. We understand that the LRC is currently studying the subject. The private member's bill discussed by the then LegCo in 1997 originally covered oral communications (in addition to telecommunications and postal communications), which would be relevant to covert surveillance. At the Committee Stage of scrutinizing the passage of the bill after Second Reading, the bill was amended to exclude oral communications, and as a result the IOCO covers only telecommunications and postal interception.

6. In April 2005, in the Li Man-tak case the District Court judge expressed the view that the covert surveillance operation in the case had been carried out unlawfully, although he eventually allowed the evidence so obtained to be admitted as evidence in the case. In view of the public concerns with such operations that had been expressed following the judge's ruling in that case, in August 2005 the Chief Executive made the Law Enforcement (Covert Surveillance Procedures) Order, and the Administration announced at the same time its intention to regulate covert surveillance operations by means of legislation. At the meeting of the LegCo Panel on Security on 4 October 2005, the Secretary for Security said that proposals for such legislation would be presented to LegCo as soon as possible within the first half of the 2005/06 legislative session.

7. In considering proposals for legislation on interception of communications and covert surveillance, we have taken into account :

- the 1996 LRC consultation paper on regulating surveillance and interception of communications;
- the 1996 LRC report on interception of communications;
- the 1997 White Bill and comments received in response to the White Bill;
- the IOCO;
- comparable legislation of other common law jurisdictions; and
- views expressed on the subject by interested parties, particularly those in exchanges that we have conducted in recent months.

The proposals put forward in this paper, so far as they relate to interception of communications are broadly in line with those in the 1996 LRC report on interception of communications and the 1997 White Bill, with modifications including those aimed at increasing safeguards in the system. A table comparing

the key elements of our proposed system and those in the 1996 LRC report, the IOCO, and the White Bill is at **Annex**.

Proposals for legislation

8. We propose that the new legislation should cover both interception of communications and covert surveillance. In approaching the two subjects, we have taken account of the following –

(a) the need for these investigative techniques to be conducted covertly in the interests of law and order and public security;

(b) the need for adequate safeguards for privacy and against abuse; and

(c) the public's expectation that new legislation regulating the use of these covert investigative techniques should be put in place as early as possible, providing for a proper balance between (a) and (b) above and a statutory basis for such investigative operations.

9. By their nature, interception of communications and covert surveillance operations have to be confidential. There is, therefore, necessarily a limit to the extent to which they may be openly discussed and publicly monitored. Nonetheless, we fully recognize the need to ensure the proper implementation of a regime whilst protecting the privacy of individuals against unwarranted intrusion. In line with international trends, we propose to introduce safeguards at different stages of such operations.

10. The main features of our legislative proposals are set out below.

Non-government parties

11. Article 30 of the Basic Law (BL30) provides that –

> *"The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communications in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences."*

It may therefore be argued that legislative proposals should provide for protection of privacy of communication not only from actions by government parties but also from actions by non-government parties.

12. The Administration accepts that there should be suitable protection against the infringement of the privacy of communications by both government and **non-government parties**. However, many interlocutors whom we have consulted have advised that given the desirability of new legislation being in place as soon as possible to regulate LEAs' conduct in this area, there is a case for dealing with government parties first and deferring non-government parties to a separate, later exercise.

13. We agree with this advice and therefore propose that we limit the current exercise and our new legislation, to cover Government parties only. It is relevant that the existing law has a number of remedies to deal with the infringement of privacy in general. For example, the collection of personal data is regulated under the Personal Data (Privacy) Ordinance (Cap. 486). The LRC has also published various reports on such related subjects as civil liability for invasion of privacy, which are being considered by the Administration. In addition, the LRC is looking into the subject of covert surveillance. The Administration will study the LRC's further recommendations carefully before considering how best to deal with the infringement of the privacy of communications by other parties.

Authorization

14. For both interception of communications and covert surveillance, we propose that authorization should only be given for the **purposes** of preventing or detecting serious crime (i.e. offences punishable with a maximum imprisonment of not less than 3 years or a fine of not less than $1,000,000 for covert surveillance, or offences punishable with a maximum imprisonment of not less than 7 years for interception of communications) or the protection of public security.

15. Even when the specified purposes apply, authorization should only be given where the **tests of proportionality and hence necessity** are met, taking into account the gravity and immediacy of the case and whether the purpose sought can reasonably be furthered by other less intrusive means. Thus applications for authorization would have to set out such information as the likely intrusion into the privacy of people other than the target and the likely benefit from the proposed operation. The applications would also have to address the possibility of the operation covering any information that may be subject to legal professional privilege.

16. We propose that authorizations granted should be for a **duration** of no longer than three months beginning with the time when it takes effect, should not be backdated, and should be renewable for periods of not exceeding 3 months each time, subject to similar criteria as for new applications.

17. We propose that it should be possible for an application for authorization or renewal to be made orally if it is not reasonably practicable for the application to be considered in accordance with the normal procedure. Such an application should be followed by a written record within 48 hours of the oral application and the authorizing authority may confirm or revoke the oral approval given. Special provisions would also be made for dealing with very urgent cases, with durations of authorization limited to 48 hours. In both **oral and very urgent application cases**, should the applications be subsequently revoked, the information gathered, to the extent that it could not have been obtained without the authorization, may be ordered to be destroyed immediately.

18. As for the **authorization authority**, we propose that all interception of communications should be authorised by judges. As for covert surveillance, there is a wide spectrum of such operations with varying degrees of intrusiveness. As in many other jurisdictions, it is necessary to balance the need to protect law and order and public security on the one hand, and the need for safeguarding the privacy of individuals on the other. More stringent conditions and safeguards should apply to more intrusive activities.

19. We therefore propose a two-tier authorization system for covert surveillance, under which authorization for "more intrusive" operations would be made by judges, and "less intrusive" operations by designated authorizing officers within LEAs. Surveillance that does not infringe on the reasonably expected privacy of individuals would not require authorization.

20. Whether a covert surveillance operation is "more intrusive" or "less intrusive" depends mainly on two criteria : whether surveillance devices are used and whether the surveillance is carried out by a party participating in the relevant communications. In general, operations involving the use of devices are considered more intrusive. On the other hand, when the use of devices involves a party participating in the relevant communications, the operation is considered less intrusive because that party's presence is known to the other parties and that party may in any case relate the discussion to others afterwards.

21. The authority for authorizing all interception of communications and the more intrusive covert surveillance operations would be vested in one of a panel of judges. Members of the panel would be appointed by the Chief Executive (CE) based on the recommendations of the Chief Justice (CJ). The panel would consist of three to six judges at the level of the Court of First Instance of the High Court. To ensure consistency and to facilitate the building up of expertise, panel members would have a tenure of three years and could be reappointed.

22. For less intrusive covert surveillance, authorization should be given by a senior officer not below a rank equivalent to that of senior superintendent of

police, to be designated by the head of the respective LEA.

23. Furthermore, we propose that applications for authorization of these covert operations should only be made by officers of specified departments. These would initially be the Police, the Independent Commission Against Corruption, Customs and Excise Department and Immigration Department. Moreover, applications to the judge (in the case of interception of communications and more intrusive covert surveillance) should only be made after clearance by a directorate officer of the LEA concerned.

Independent oversight authority and complaints handling

24. We propose to establish an **independent oversight authority** to keep under **review LEAs' compliance** with the provisions of the legislation and any code of practice (see para. 31 below). There would also be an **independent complaints handling mechanism** for receiving and investigating complaints against unlawful interception of communications or covert surveillance and awarding compensation. While there may be arguments for separate authorities to perform the oversight and complaints handling functions, our thinking is that the oversight authority could also assume the complaints handling function. The authority, entitled the "Commissioner on Interception of Communications and Surveillance" ("the Commissioner"), is proposed to be a sitting or retired judge not below the level of the Court of First Instance of the High Court, to be appointed by CE. Again CE would consult CJ for recommendations. The term of appointment is proposed to be three years and renewable.

25. We envisage that the Commissioner would conduct sampling audits in carrying out his review function. He would examine compliance and propriety in respect of the information supplied in an application for authorization, the execution of the authorization and the implementation and observance of various safeguards to protect the operation and information gathered. On detecting any irregularities in the course of his review, the Commissioner would be able to bring the matter to the attention of the head of the LEA concerned and request corresponding action to be taken. The head of the LEA would have to report to the Commissioner what action he has decided to take and the reasons. Where he considers it necessary, the Commissioner would also be able to refer such cases to CE or the Secretary for Justice (where, for example, criminal proceedings may be required).

26. The Commissioner, in performing his functions, should have access to any relevant official document. Public officers concerned would be required by law to support and cooperate with the Commissioner in the performance of his statutory functions. LEAs would also be required to report to the Commissioner all instances of non-compliance with the legislation, terms of authorization or code

of practice.

27. The Commissioner would be required to submit **annual reports** to CE on his work, and CE would cause the reports to be tabled in the Legislative Council. The annual report should include information covering interception of communications and covert surveillance respectively, such as the number and duration of authorizations / renewals granted / denied, major categories of offences involved, etc.

28. As far as the complaint mechanism is concerned, a person who believes that any communication sent to or by him has been intercepted by the LEAs, or that he himself is the subject of any covert surveillance operation by the LEAs, would be able to apply for an examination under the mechanism. The complaints authority would consider the complaint by applying the test applicable in a judicial review. If the complaints authority concludes, after examination of the case, that an interception of communications or covert surveillance operation has been carried out by an LEA on the applicant, but was not duly authorized under the legislation where it should have been, the authority may find the case in the applicant's favour. The authority would also be empowered to order the payment of compensation to the applicant. Should the complaints authority detect any irregularities in the course of handling a complaint, the authority may bring the case to the attention of the head of the LEA concerned, as well as the CE or the Secretary for Justice where appropriate.

Regular internal reviews

29. In addition to reviews to be conducted by the Commissioner, the head of LEA concerned would be required to make arrangements to keep under regular review the compliance of officers of the department with authorizations given under the legislation. Moreover, arrangements would be made for officers at a rank higher than those held by the authorizing officers of the department to keep under regular review the exercise and performance by the authorizing officers of the powers and duties conferred or imposed on them by the legislation in respect of less intrusive covert surveillance operations.

Discontinuation of operations

30. Where, before an authorization made ceases to be in force, the officer in charge of the operation is satisfied that the required conditions for obtaining the authorization are no longer satisfied or the purpose for which the authorization was granted has been achieved, he would be required to cease the operation as soon as practicable, and notify the relevant authorizing authority of the discontinuation of the operation. The authorizing authority would then revoke the authorization.

Code of practice

31. A code of practice for the purpose of providing guidance to law enforcement officers would be prepared under the legislation. We propose that the code be made by the Secretary for Security. The Commissioner may recommend amendments to the code. Any breach of the code of practice would need to be reported to the Commissioner.

Handling and destruction of materials

32. The legislation would require arrangements to be made to ensure that materials obtained by interception of communications and covert surveillance are properly handled and protected. These include keeping the number of persons who have access to the products of interception and surveillance and their disclosure to a minimum, and requiring that such products and any copies made are destroyed or otherwise disposed of as soon as their retention is no longer necessary.

Evidential use

33. We have for a long time adopted the policy of not using telecommunications intercepts as evidence in legal proceedings in order to, among other things, protect privacy. At the same time, intercepts are destroyed within a short time. This ensures an equality of arms between the prosecution and the defence as neither side may use intercepts as evidence. In addition, it minimizes the intrusion into the privacy of innocent third parties through keeping the records which will be subject to disclosure during legal proceedings.

34. On the other hand, covert surveillance products are used as evidence in criminal trials from time to time. As covert surveillance is usually more event and target specific, the impact on innocent third parties and hence privacy concerns are less.

35. We propose that the current policy and practice in respect of evidential use above should be codified in law. The legislation should, therefore, expressly disallow all telecommunications intercepts from evidential use in proceedings. As a corollary, such materials would not be made available to any party in any proceedings, and questions that may tend to suggest the occurrence of telecommunications interception should also be prohibited from being asked in such proceedings.

Consequential amendments

36. The existing provisions governing interception of postal communications, namely section 13 of the Post Office Ordinance, would be repealed, while the provision governing interception of telecommunications under section 33 of the Telecommunications Ordinance would be retained and suitably amended to cater for the operations of, for example, the Office of the Telecommunications Authority in detecting unlicensed service operators. The Interception of Communications Ordinance would be repealed.

Security Bureau
February 2006

Annex

Comparison of the Administration's Proposals on Interception of Communications and Covert Surveillance with the Proposed Regulatory Regime under the 1996 LRC Report, 1997 White Bill and the Interception of Communications Ordinance (IOCO)

	Current Proposals	1996 LRC Report	White Bill	IOCO
Coverage	- Covert surveillance - Interception of telecommunications - Interception of postal articles	- Interception of telecommunications - Interception of postal article	- Interception of telecommunications (*excluding* messages carried by computer network) - Interception of postal articles	- Interception of telecommunications - Interception of postal article
Applicability	Government parties only[1]	Both government and non-government parties	Both government and non-government parties	Both government and non-government parties
Grounds for authorization	Preventing or detecting serious crime[2] or protecting public security.	Prevention or detection of serious crime[2] or safeguarding of public security in respect of Hong Kong	Prevention/investigation/detection of serious crime[2], or for the security of Hong Kong	Prevention or detection of serious crime[2], or in the interest of security of Hong Kong
Authorization Authority	For interception and more intrusive covert surveillance : 3-6 designated panel judges of the Court of First Instance of the High Court For less intrusive covert surveillance : Senior officers (equivalent in rank to senior superintendent or above) of specified law enforcement	For interception: Judges of the Court of First Instance of the High Court	For interception: Not more than 3 designated judges of the Court of First Instance of the High Court	For interception: Judges of the Court of First Instance of the High Court

---

1 Without prejudice to existing legislative provisions under the Telecommunications Ordinance (Cap 106) on willful interception (sections 24 and 27) or unauthorized opening of postal articles under the Post Office Ordinance (Cap 98) (sections 28 and 29).

2 For interception of communications , serious crime refers to offences punishable with a maximum imprisonment of not less than 7 years in the contexts of our proposals, the White Bill and IOCO. On the other hand, the 1996 LRC Report recommends including offences punishable with a certain maximum imprisonment, to be determined by the Administration. Regarding covert surveillance, serious crime in our proposals refers to offences punishable with a maximum imprisonment of not less than 3 years or a fine of not less than $1,000,000.

3 The specified departments are the Police, Independent Commission Against Corruption, Immigration Department and Customs and Excise Department.

	Current Proposals	1996 LRC Report	White Bill	IOCO
	departments[3]			
Who may apply for authorizations	For interception and more intrusive covert surveillance : Any officers of specified departments[3] with prior approval by directorate officers For less intrusive covert surveillance : Any officer of specified departments[3]	For interception: Senior officers to be determined by the Administration	For interception: Directorate officers to be authorized by the Chief Executive	For interception: Designated group of officers of specified departments[4]
Maximum duration of authorization	3 months. Renewals allowed	90 days. Renewals allowed	6 months. Renewals allowed	90 days. Only one renewal allowed
Urgent cases	For interception and more intrusive covert surveillance: Approved by Head of Department, followed by written application to a panel judge within 48 hours. Destruction of material if authorization subsequently revoked	For interception : Approved by designated directorate officer, followed by written application to the court within 48 hours. Destruction of material if authorization subsequently rejected	For interception : Approved by an authorized directorate officer, followed by written application to designated judges in 2 working days. Destruction of material if authorization subsequently rejected	For interception : Approved by Head of Department, to be followed by written application to the court within 48 hours from beginning of interception. Destruction of material if authorization subsequently rejected
Evidential use	For telecommunications interception: No evidence shall be adduced and no question shall be asked in court proceedings which tends to suggest an authorized interception has taken place For postal interception and covert	For telecommunications interception: No evidence shall be adduced and no question shall be asked in court proceedings which tends to suggest an authorized or unauthorized interception	For both telecommunications and postal interception: No evidence shall be adduced and no question shall be asked in court/tribunal proceedings which tends to suggest that an authorized or unauthorized interception	For interception : Evidential use allowed. Prosecution needs to prove beyond reasonable doubt that the material was obtained in accordance with the Ordinance if challenged

[4] Under IOCO, the specified departments are the Police, Independent Commission Against Corruption, Immigration Department, Customs and Excise Department and the Correctional Services Department.

	Current Proposals	1996 LRC Report	White Bill	IOCO
	surveillance: Usual evidential rules apply	For postal interception : Usual evidential rules apply		
Oversight	Yes – serving or retired judge at the Court of First Instance level of the High Court or above to serve as oversight authority. To review compliance with legislative requirements and handle complaints	Yes – sitting or former Justice of Appeal to serve as supervisory authority. To review compliance with legislative requirements and handle complaints	Yes – Justice of Appeal to serve as supervisory authority. To review compliance with legislative requirements and handle complaints	No oversight mechanism
Reporting to Legislative Council (LegCo)	Annual reports by oversight authority to the Chief Executive (CE) to be tabled at LegCo	Annual reports by supervisory authority to LegCo	Annual reports by supervisory authority to CE to be tabled at LegCo	No annual reports to LegCo. LegCo may require the Secretary for Security to provide specified information from time to time
Remedies	Oversight authority may order payment of compensation to complainants Oversight authority may refer irregularities to CE, the Secretary for Justice (SJ) or Head of Department as appropriate	Revocation of authorization under specified circumstances Supervisory authority may order compensation to complainants Supervisory authority may refer case to SJ (to consider prosecution)	Quashing of authorization Supervisory authority may order compensation to complainant	Court may grant relief by making an order (a) declaring interception or disclosure unlawful, (b) that damages be paid to the aggrieved person, or (c) in the nature of an injunction
Other safeguards	Detailed requirements on record keeping, disclosure, handling and destruction of materials Regular internal reviews by departments Code of practice for law enforcement officers to be issued by the Secretary for Security. It will be publicly available	Requirements on record keeping, disclosure, handling and destruction of materials	Requirements on record keeping, disclosure, handling and destruction of materials	Requirements on record keeping, disclosure, handling and destruction of materials Where no charge is laid against the target within 90 days of the termination of a court order, the court would notify the person that his communications have been intercepted

February 2006

Annex C

Interception of Communications and Covert Surveillance
Response to issues raised at the Panel on Security

- Information Paper to Panel on Security of LegCo on 16 February 2006

- Information Paper to Panel on Security of LegCo on 21 February 2006

- Information Paper to Panel on Security of LegCo on 2 March 2006

For information
16 February 2006

Legislative Council Panel on Security

Interception of Communications and Covert Surveillance

Response to issues raised by Members at the meeting of 7 February 2006

Introduction

This paper sets out the Administration's response to issues raised by Members at the meeting of the Panel on Security of the Legislative Council (LegCo) on 7 February 2006. The numbering of items follows that set out in the revised list of issues attached to the letter of 9 February 2006 from the Clerk to Panel.

Responses to issues raised

Item 1 : To clarify whether the protection of public security includes the protection of national security.

2. The question was asked in relation to Article 23 of the Basic Law (BL23). As the Secretary for Security indicated at the meeting of the Panel on Security on 7 February 2006, the present exercise is unrelated to the BL23 exercise. No interception of communications or covert surveillance would be carried out for offences under BL23 that have yet to be created.

3. We have referred to "public security" in our proposals as it is the term used in Article 30 of the Basic Law. As can be seen from the 1996 Law Reform Commission (LRC) Report on interception of communications (the 1996 LRC report), the 1997 White Bill on Interception of Communications and the 1997 Interception of Communications Ordinance (IOCO), the approach generally is to leave

the term "public security" undefined so that security cases are considered and justified on their own individual circumstances. All applications must satisfy the tests set out in the law. All interceptions and more intrusive covert surveillance operations would have to be approved by a member of the panel of judges. In addition, all such operations would be subject to oversight by the proposed Commissioner on Interception of Communications and Surveillance (the Commissioner).

Item 2 : To clarify whether Mainland public security authorities and State security organs are within the meaning of non-government parties under the proposed new legislation.

4. During this first stage of the exercise, we seek to authorize and regulate the conduct of our law enforcement agencies (LEAs) and we would in fact be specifying those departments under the law. Non-government entities would not be dealt with at this stage under our current proposals. For similar activities of parties other than those of the Hong Kong Special Administrative Region Government, they are subject to current laws (statutes and common law) that apply to all persons in Hong Kong (please see paragraph 15 below). They will also be subject to any future laws that may be made in this and other related areas. In this connection, the following studies the LRC has done or is doing may be relevant –

- its 1996 report on interception of communications proposing criminal offences for certain activities by both government and non-government parties;
- its 2004 report on civil liability for invasion of privacy proposing to create civil liabilities for the invasion of privacy;
- its 2004 report on privacy and media intrusion proposing to establish an independent and self-regulating press commission for the protection of privacy, to handle complaints against the press and draw up a Press Privacy Code for the practical guidance of the press; and
- its 2000 report on stalking proposing the creation of a criminal offence for stalking.

These issues may be dealt with separately.

Item 3 : To consider providing in the legislation that reasons for interception of communications or covert surveillance should be included in the application for judicial authorization, and such application should be made by way of an affidavit.

5. We agree that all applications for authorization should be supported by sufficient reasons, and propose to list the information required in the legislation. As regards the form, our current thinking is that an affidavit would be required for judicial authorizations and a declaration would be required for executive authorizations.

Item 4 : To advise whether the renewal of judicial authorization would be indefinite, and if so, the justifications for that.

Related comments from the Criminal Law & Procedure Committee of the Law Society : The Committee has reservations on the 3 months' duration of authorizations and considers this to be too long for the initial authorization.

6. The three-month period proposed is the maximum duration that may be granted. The actual duration of the renewal would depend on the circumstances of each case and would have to be determined by the approving authority. Like a first-time application, an application for renewal would have to meet all the requirements regarding purpose, proportionality and necessity. In addition, it has to set out the benefits so far accrued from the operation and why a renewal is required.

7. Moreover, as with first-time authorizations, we would provide that once the purpose of the interception of communications or covert surveillance has been achieved or the conditions for the continuance of the authorization no longer apply, the operation has to be discontinued even if the renewal has not expired. The renewal then has to be revoked.

8. The maximum duration of three months is the same as that

recommended in the 1996 LRC report and under the IOCO, and is the same as or less than the maximum duration allowed in Australia and the United Kingdom (UK) (ranging from 90 days to six months, depending on the nature of the cases).

9. Imposing a limit on the number of renewals could unnecessarily restrict the ability of LEAs to combat such crime as syndicated crime that usually requires a longer period of monitoring.

10. Paragraphs 6.125 to 6.129 of the 1996 LRC report discuss the duration question. They are extracted at **Annex A** for Members' ease of reference.

Item 5 : To explain the circumstances under which covert surveillance will be carried out by law enforcement agencies.

Item 6 : To explain how to differentiate between "more intrusive" operations and "less intrusive" operations under the two-tier authorization system for covert surveillance.

Item 7 : To illustrate by way of examples how the two-tier authorization system for covert surveillance works.

11. A note setting out the circumstances under which judicial and executive authorizations would be required in the case of covert surveillance operations is at **Annex B**.

12. We consider that the present scheme would provide very clear tests as to the circumstances under which different authorizations are required. Where there has been a change of circumstances requiring a different level of authorization, the appropriate authorization would need to be sought before an intended operation may be carried out. If both "more intrusive" and "less intrusive" surveillance is involved in a single operation, then judicial authorization would be sought.

13. Both types of covert surveillance would come under the purview of the Commissioner and would be subject to the same

safeguards in respect of protection of products, etc. Furthermore, there are internal review mechanisms to ensure compliance with the relevant requirements. There is therefore little room for abuse.

Item 8 : To advise on the consequences of illegal covert surveillance conducted by law enforcement agencies.

Item 9 : To consider adding penalty provisions for non-compliance with any code of practice made under the proposed legislation.

14. We have proposed that the current exercise be limited to Government entities. This means that non-Government parties would not be subject to the regulation proposed. It would create an anomaly if, for the same conduct, law enforcement officers but not others would be subject to a new criminal offence. We will consider the need for introducing new criminal offences at the next stage. Under our proposal, a breach under the proposed legislation would be subject to disciplinary action, and this would be stipulated in the code of practice. An officer who deliberately conducts operations without due authorization might also commit the common law offence of misconduct in public office. In addition, any non-compliance would be subject to the scrutiny of the Commissioner, who may report such cases of irregularity to the heads of department and to the Chief Executive (CE), and who would handle complaints. Statistics on such cases would also be provided to CE in the Commissioner's annual report, which would be tabled in LegCo. These are powerful measures to ensure that LEAs and their officers will comply with the law and the applicable procedures.

15. Separately, all public officers have to observe the full range of existing laws. For example, the Telecommunications Ordinance provides for various offences in relation to the wilful interception of messages (sections 24) and damaging telecommunications installations with intent (section 27). The Post Office Ordinance has provisions governing the unauthorized opening of postal packets (sections 27 and 29). Other laws such as the Personal Data (Privacy) Ordinance may also be relevant. For a fuller summary of existing laws that may be applicable, please see Chapter 2 of the 1996 LRC report.

Item 10 : To advise whether the code of practice made under the legislation is subsidiary legislation.

16. The basic principles of the regime would be set out in the law. Amendments to these would necessarily have to be passed by LegCo. We do not consider it advisable for the Code of Practice covering operational details, which may need to be changed from time to time, to be made statutory. Our proposed legislation would stipulate that the Commissioner may make recommendations to the Secretary for Security on the Code or propose amendments thereto, thereby providing a considerable degree of oversight in respect of the content of the Code. Furthermore, the Code would be published and hence subject to public scrutiny.

Item 11 : To provide a list of offences where authorization should be given for covert surveillance and interception of communications respectively.

Item 12 : To provide information on the interception of communications and covert surveillance conducted by law enforcement agencies in terms of categories of offences.

17. We propose to set the threshold of the seriousness of offences by reference to an objective test – the maximum penalty for the offence. This approach is similar to that adopted in the 1996 LRC report, the 1997 White Bill and the IOCO. For covert surveillance, the threshold is offences with a maximum imprisonment term of at least 3 years or with a maximum fine of at least $1 million, and for interception of communications, offences with a maximum imprisonment term of at least 7 years. For comparison, the following summarizes the thresholds in the UK, Australia, and the United States (US) –

(a) the UK : in respect of interception and intrusive surveillance, offences for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to three years of imprisonment or more, or crimes that involve the use of violence, results in substantial financial

gain or is conducted by a large number of persons in pursuit of a common purpose;

(b) Australia : in respect of telecommunications interception, offences punishable by imprisonment for at least 7 years; in respect of surveillance, "relevant offences" include those punishable by imprisonment of 3 years or more, a few other specific offences, and offences prescribed by the regulations; and

(c) the US : in respect of interception of telecommunications and use of electronic surveillance devices, the list of offences enumerated in the Federal Wiretap Act s. 2516, where some offences are punishable by imprisonment for more than one year; in respect of interception of postal articles, all criminal activities.

18. Interception is considered to be a highly intrusive investigative technique and therefore a higher threshold is necessary. On the other hand, there is a wide spectrum of covert surveillance operations with varying degrees of intrusiveness. Also, since surveillance operations in general can be more specific in terms of location, timing and event, they are less intrusive. On this basis, it seems reasonable to impose a lower threshold on the crimes over which such investigative technique could be deployed.

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.

20. It is very important to bear in mind that the threshold is but an initial screen. Whether interception or covert surveillance may be authorized in each case has to be assessed against the proportionality and necessity tests.

Item 13 : To provide statistics on the "more intrusive" and "less intrusive" covert surveillance operations carried out by law enforcement agencies.

21. We have tried to see if it is possible to compile the relevant figures, but have found it very difficult to do so. The existing system is very different from the proposed one. Previously there have been no uniform reporting requirements across the LEAs for publication, and no classification as presently proposed. As a result, we have not adopted a uniform system of keeping past statistics, and it would be impracticable to work out the figures post-hoc. With interception of communications, in line with long-standing policy, the records are destroyed within a fairly short time to protect privacy and are no longer available. For covert surveillance, even if the records are still available, a mammoth effort would be required to go over the records for a number of years to prepare the figures for them to be meaningful.

22. Looking ahead and for the purpose of consideration of our proposed regime, it is relevant that :

(a) there would be uniform classification of operations, which would enable the preparation of uniform statistics; and

(b) the proposed legislation would specify information that has to be included in the proposed Commissioner's report to CE, which would be tabled in LegCo. Such information would include the number of authorizations and renewals issued, the number of applications that have been refused and a summary of reviews conducted by the Commissioner, etc.

Item 14 : To reconsider whether the panel of judges authorizing interception of communications and the more intrusive covert surveillance operations should be appointed by the Chief Executive.

23. Vesting the approving authority for interception of communications and the more intrusive covert surveillance in a panel of High Court judges would –

- ensure that the cases would be considered by senior judges with considerable judicial experience;
- allow the building up of expertise in dealing with the usually highly sensitive cases;
- facilitate the application of consistent standards in dealing with the cases; and
- facilitate the Judiciary in planning and deploying judicial resources, for example, in the listing of cases.

We have consulted the Judiciary and the Judiciary's position is that the proposal is acceptable.

24. Prior to making the appointments, CE would ask the Chief Justice (CJ) for recommendations. In other words, CE would only appoint someone recommended by CJ. The term of appointment would be fixed at three years, and we propose that CE would only revoke an appointment on CJ's recommendation and for good cause. We have consulted the Judiciary, and the Judiciary's position is that the proposal is acceptable.

25. Judges appointed to the panel will receive no advantages from that appointment. They will continue to be judges and whatever they do while on the panel will in no way affect their continued eligibility as judges. That they are appointed by CE to the panel therefore would give no positive or negative incentives that might affect their independence when carrying out their duties as judges on the panel.

26. Designating selected judges to deal with different types of case

is not uncommon either in Hong Kong or overseas. For example, the Judiciary practises a listing system designating certain judges to handle certain types of case. In the US, applications for foreign electronic surveillance orders may only be made to one of 11 federal judges. The Australian experience also indicates that not all judges are prepared to take up the responsibility.

27. The proposed appointment arrangement takes into account the above considerations; and would be comparable with the arrangement elsewhere for the appointment to be made by a senior member of the government. For example, in Australia, a Minister nominates the members of the Administrative Appeals Tribunal to approve interception of communications. In the UK, the Prime Minister appoints the Surveillance Commissioner for approving intrusive surveillance operations.

Item 15 : To consider establishing a committee as an independent oversight authority to keep under review law enforcement agencies' compliance with the provisions of the legislation regulating interception of communication and covert surveillance and any code of practice made under the legislation.

28. Our recommendation is in line with the recommendation in the 1996 LRC report in this respect. The Commissioner would be responsible for both ensuring compliance and examining complaints. Given the nature of work involved and to underline the independence of the authority, we consider that a person with judicial experience at a senior level should be appointed. We therefore propose that the law stipulate that either serving or retired judges at or above the level of the Court of First Instance of the High Court may be appointed as the authority.

29. Appointing a single person as a statutory authority is a common practice either in Hong Kong or overseas. For example, in Hong Kong the Ombudsman and the Privacy Commissioner are statutory authorities. In the UK, the oversight authority is the Interception of Communications Commissioner. In Australia, the Ombudsman performs the oversight

function. As with the Privacy Commissioner or the Ombudsman, our proposed Commissioner will be supported by sufficient staff for him to discharge his functions.

Item 16 : To advise whether any person whose communication sent to or by him has been intercepted by the law enforcement agencies or he himself is the subject of any covert surveillance operation would be informed of such activities conducted, and if not, the justifications for that.

30. In the 1996 LRC report, the LRC explained why it concluded against notification of targets of interception of communications. In essence, the LRC recognized the conflict between notification and the purposes of interception, which is necessarily clandestine. Notification could affect the operational effectiveness of LEAs. The prolonged retention of intercepted material arising from a notification requirement would have its own privacy risks. In addition, if the notification requirement is to be applied meaningfully, it will require the relevant authority to make an informed decision as to whether notification should be effected and the extent of information to be given to the target on a case by case basis. The resource implications are obvious. Also, destruction of the intercepted material prior to notification would largely destroy the basis of the notification mechanism. In line with the LRC's recommendation that material obtained through an interception of telecommunications shall be inadmissible in evidence, if intercepted material were destroyed and inadmissible in court, the risk of dissemination, and hence the risk to privacy, could be reduced to the minimum. We agree with the LRC's analysis and recommendations.

31. We note that neither the UK nor Australia has a notification arrangement. Given our policy in respect of the handling of telecommunications intercepts (see paragraphs 35 to 36 below), there is all the more reason not to notify the target. In covert surveillance cases where the product of covert surveillance would be able to be introduced into court proceedings, the product could be introduced into evidence or be disclosed as unused material, and the aggrieved person would be able to challenge it in court.

Item 17 : To explain, quoting examples, the circumstances under which oral and very urgent applications (referred to in paragraph 17 of the Administration's paper for the meeting on 7 February 2006) would be made.

32. Oral applications could apply to both judicial and executive authorizations. They may be made in circumstances where a written application is not feasible, e.g., where a panel judge may be contacted by telephone but a hearing involving the applicant may otherwise not be feasible. Emergency authorizations apply only to cases which would otherwise require judicial authorization. We propose that the application should be made to the respective head of department who will not grant the authorization or renewal sought unless he is satisfied that it is not reasonably practicable, having regard to the urgency of the particular case, for the application to be submitted to the judge in accordance with the normal procedure. However, within 48 hours the application for confirmation must be made to a judge, who may revoke the approval. And as an additional safeguard, each case where the judge refuses to confirm the authorization would have to be reported to the Commissioner

33. The circumstances under which emergency applications could be considered should include imminent risk of death or serious bodily harm, substantial damage to property, serious threat to public security and loss of vital evidence. It is important for such procedure to be provided for in law so that the LEAs could arrange for emergency operations in well justified cases. We envisage that in practice emergency authorizations would only be resorted to sparingly and we anticipate that the Commissioner would wish to review such cases to ensure that the emergency application procedure is not abused.

Item 18 : To provide a written response to the issues raised in the letter dated 7 February 2006 from The Law Society of Hong Kong.

34. The response of the Administration set out above should address all issues covered in the Law Society's letter save for the issue on evidential use of telecommunication intercepts. ***The Society has***

indicated that its Criminal Law & Procedure Committee has reservations on the proposed destruction of material. They are of the view that the normal rule of disclosure should apply and the defence should have a right of disclosure to any unused material.

35. The LRC has set out its analysis on the evidential use and admissibility of telecommunications intercepts in the 1996 LRC report. The relevant extract is at **Annex C**. We agree with the LRC's analysis and recommendations.

36. Since neither the prosecution nor the defence may adduce any evidence from telecommunications intercepts, there is equality between the two sides in this respect. In a recent ruling of a case (in the case of Mo Yuk-ping on 23 August 2005), the court was satisfied that the policy adopted by the Government of allowing telecommunications intercepts for intelligence gathering only and thereafter requiring the destruction of the product to be rational, striking an acceptable balance between various competing interests. *[re: para. 83 and 88 of Judge Wright's ruling]* Having said that, to cater for any exceptional cases, we would also provide in the legislation that disclosure should be made to the judge where the fairness of the trial so requires.

37. Safeguards are provided at different stages of the process to ensure fairness. All authorizations for interception operations would be given by members of a panel of judges. There are also a number of safeguards in our proposals regarding, for example, the need to protect the confidentiality of intercepts products, limiting access to these materials, etc. The execution of the authorization, including the compliance with safeguards, would also be subject to review by the Commissioner.

Security Bureau
February 2006

Annex A

Relevant Extract from the 1996 LRC report on interception on communications

Duration and renewal of warrants

6.125 Having determined the matters that must be made out to justify the issue of a warrant, the question of the warrant's duration requires consideration. We recommended in the consultation paper that a warrant should be issued for an initial period of 60 days. The Bar Association agreed that the period should be no longer than that. The Hon James To proposed that the period should be not more than 30 days so as to reflect the principle that interception is a last resort and should not be used unless it is absolutely necessary. Two other respondents commented that 60 days is too short and would like to see the duration extended to six months. Their concern is that investigations are often protracted and applying to court for renewal every two months would create inconvenience to the law enforcement agencies.

6.126 We are conscious that any decision on the length of warrant must be arbitrary. But the length is less of an issue than the arguments put forward by the applicant. If the applicant has a strong case, he can always come back to the court and apply for renewal. Nonetheless, we are concerned that the court might be burdened with unnecessary applications for renewal if the duration is as short as, say, 30 days.

6.127 We conclude that 90 days should suffice for both crime and public security. A similar period should govern extensions. In coming to this conclusion, we have considered the experience overseas. The position in other jurisdictions is summarised as follows:

(a) *Australia*

- 90 days if a criminal offence is involved;[1]
- Six months if the activities concerned are prejudicial to security.[2]

---

1 Telecommunications (Interception) Act 1979 (Australia), section 49(3).
2 Telecommunications (Interception) Act 1979 (Australia), section 9(5).

(b) *Canada*

- 60 days under the Criminal Code;[3]
- 60 days or 1 year under the Canadian Security Intelligence Service Act 1984.[4]

(c) *Germany*

- Three months.[5]

(d) *New Zealand*

- 30 days for investigation of organised crime.[6]

(e) *South Africa*

- 90 days.[7]

(f)*United Kingdom*

- 60 days under the Interception of Communications Act 1985;[8]
- Six months under the Security Service Act 1989[9] and the Intelligence Services Act 1994.[10]

(g) *United States*

- 30 days.[11]

6.128 We have considered adoption of an upper limit to the number of extensions given, but have rejected this because each extension would have to be justified on the prescribed criteria.

---

3 Section 186(4)(e).
4 Section 21(5).
5 Act on Restriction of the Secrecy of Mail, Posts and Telecommunications 1968, section 5(3).
6 Crimes Act 1961, section 312D(3).
7 Interception and Monitoring Prohibition Act 1992, section 3(3).
8 Section 4. It provides that warrants shall be issued for an initial period of 2 months and thereafter require renewal, also for a period of 2 months (but with provision for 6 months). Renewal requires that the Minister considers that the warrant "continues to be necessary" for the relevant purpose under section 2.
9 Section 3(4).
10 Section 6(2).
11 Wiretap Act, section 2518(5).

6.129 **We recommend that a warrant should be issued for an initial period not exceeding 90 days and that renewals may be granted for such further periods of the same duration where it is shown (according to the same criteria applied to the initial application) to continue to be necessary.**

* * * * * *

Annex B

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

<u>Definition of covert surveillance</u>

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).

Annex C

Relevant Extracts from the 1996 LRC report on interception on communications : Evidential Use and Admissibility

Admissibility of material obtained through interception of communications carried out pursuant to a warrant

7.23 The adoption of section 6 of the 1985 Act will have the result that evidence of the fruits of *authorised* interception of telecommunications can never be produced in court. The intercepted material and the copies thereof must be destroyed once its purpose (e.g. the prevention or detection of crime) has been served. However, a party might be in breach of the requirement to destroy the material and seek to adduce it in evidence. Further, the statutory requirements for destruction would not apply to material obtained by an authorised interception of communications other than telecommunications, or an interception which was not authorised by the court.

7.24 Under general common law principles, the admissibility of evidence is solely determined by the relevance of the evidence. The court has no power to exclude evidence merely because the judge disapproves of the way in which it was obtained, as, for example, where evidence was obtained unfairly or by trickery.[12] There is, however, a judicial discretion to exclude evidence if its prejudicial effect exceeds its probative value. The court also has inherent jurisdiction to make orders which are necessary to ensure a fair trial.

7.25 In determining whether to admit intercepted material in evidence, we need to take into account the probative value of the material and the privacy risk involved. High quality evidence collected by means which pose a low privacy risk should be admissible but low quality evidence collected by means which pose a high privacy risk should be inadmissible. Other factors include the purpose of the interception, the duration of the warrant, and the amount of relevant and irrelevant information obtained from the interception.

---

[12] *R v Cheung Ka-fai* [1995] HKLR 184 at 195. The test of admissibility of evidence in Hong Kong is governed by the common law as expressed in *R v Sang* [1980] AC 402 at 432-3.

7.26 The sub-committee initially considered that intercepted material pertaining to the period preceding the laying of the charge should be admissible in the subsequent prosecution. Restricting the admissibility of evidence obtained as a result of an interception would have far-reaching results. It would mean that even if an interception reveals the sole evidence of a serious offence, that evidence may not be adduced. Similarly, evidence which assists an accused, such as an attempt to fabricate evidence against him, may not be adduced if it was obtained by interception, even though the interception was authorised by the court.

Material obtained through interception of telecommunications

7.27 While evidence arising from interception of telecommunications is not usually admitted in Hong Kong, in a recent major drug case it was.[13] We note that the laws of the United States,[14] Canada,[15] and Australia[16] regulating the interception of telecommunications all countenance the admission of lawfully intercepted material as evidence in prosecutions**.**

7.28 We recommended at the beginning of this chapter that material obtained by an interception of telecommunications should be destroyed as soon as its prescribed purpose has been fulfilled. Admitting in evidence material obtained through an interception of telecommunications would require its retention for this purpose. This would run counter to our recommendation on destruction of intercepted material. It also gives rise to the problem of disclosure of unused material to the defence. Generally, only a small part of the intercepted material would be used by the prosecution as evidence. But since the prosecution is under a duty to disclose all material information, all unused material would probably have to be made available to the defence.[17]

7.29 It is true that the court may impose appropriate conditions. For example, defence counsel may have to undertake not to divulge the contents of tapes played to them. But use of intercepted material as evidence will necessarily compound the invasion of privacy entailed in the original intrusion. There is always a risk of *public* dissemination of personal information contained in the intercepted communications.

---

13 *R v Cheung Ka-fai* [1995] HKLR 184. The calls in that case were intercepted by the Royal Canadian Mounted Police.

14 Wiretap Act, sections 2515 and 2518(9) & (10)(a).

15 Criminal Code, section 189(5). Notice of intention to introduce evidence of lawfully intercepted communications must be given to the accused.

16 Telecommunications (Interception) Act 1979, section 74.

17 *R v Preston* [1993] 4 All ER 638 at 664. The test for whether unused material should be disclosed by the prosecution to the defence is materiality, not admissibility.

Furthermore, the present legal status of unused material is vexed and is subject to a number of appeals.

7.30 A further complication which is avoided by prohibiting the use of intercepted material as evidence arises from the application of public interest immunity.

7.31 In view of the risk of public dissemination of intercepted information and the difficulties with disclosure of unused material, the sub-committee recommended in the consultation paper that material obtained through an interception of communications should be inadmissible as evidence, regardless of its relevance.

7.32 Implementing the recommendation in the consultation paper necessitates the adoption of a provision similar to section 9 of the United Kingdom Interception of Communications Act 1985. This section prohibits any reference to authorised or unauthorised interception of telecommunications and mail. Subsections (1) and (2) state:

> *"(1) In any proceedings before any court or tribunal no evidence shall be adduced and no question in cross-examination shall be asked which (in either case) tends to suggest -*
>
> *(a) that an offence under section 1 above has been or is to be committed by any of the persons mentioned in subsection (2) below; or*
>
> *(b) that a warrant has been or is to be issued to any of those persons.*
>
> *(2) The persons referred to in subsection (1) above are -*
>
> *(a) any person holding office under the Crown;*
>
> *(b) the Post Office and any person engaged in the business of the Post Office; and*
>
> *(c) any public telecommunications operator and any person engaged in the running of a public telecommunication system."*

7.33 It appears that section 9(1) would not prevent the admission of evidence and cross-examination in the exceptional cases where there can be an interception without an offence being committed (e.g. because of consent) where no warrant is in existence.

7.34 The United Kingdom Government hoped that by making intercepted material generally inadmissible in legal proceedings, it would ensure that interception could be used only as an aspect of investigation, not of prosecution.[18] However, the Court of Appeal in *Effik* held that section 9 does not provide that evidence obtained as a result of an interception would be inadmissible:

> *"The forbidden territory is drawn in a much narrower fashion. And there is a logical reason for the narrow exclusionary provision. That is the reflection that it cannot be in the public interest to allow those involved in espionage or serious crime to discover at a public trial the basis on which their activities had come to the notice of the Police, the Customs and Excise or the Security Services, such as, for example, by questions designed to find out who provided the information which led to the issue of the warrant. So interpreted section 9(1) makes sense. And it would make no sense to stretch that language to become a comprehensive exclusion of all evidence obtained as a result of any interception."*[19]

7.35 The Court of Appeal in *Preston* agreed that section 9 does not operate to render inadmissible in evidence the contents of the intercepts. However, the effect of a literal application of the language of section 9(1) would, other than possibly in the most exceptional case, be to prevent any material derived from an interception being adduced in evidence. The court explained:

> *"In order to lay the groundwork for material to be admissible in evidence the manner in which the material has been obtained will normally have to be given in evidence in court and this will in turn tend to suggest either an offence under section 1 has been committed or a warrant has been issued which therefore contravenes section 9. It is this evidence of how the material was obtained which is the 'forbidden territory' and the fact that it should not be adduced in evidence will also usually prevent the material which was obtained as a result of the interception being given in evidence."*[20]

---

18 *Interception of Communications in the United Kingdom* (Cmnd 9438, 1985), clause 12(f).
19 *R v Effik* (1992) 95 Cr App R 427 at 432.
20 *R v Preston* (1992) 95 Cr App R 355 at 365.

7.36 The result is that it is normally not possible to adduce any evidence obtained as a result of an interception to which the 1985 Act applies. Such a prohibition would cover not only the fruits of interception but also the manner in which the interception was carried out. But if the parties were by agreement or admission to put the material before the court, it appears that there is nothing in section 9 to prevent this.[21]

7.37 In Hong Kong there is no bar to the defence raising the issue of interception, provided it is relevant to the case. In practice, it is extremely rare for material obtained through interception of telecommunications to be used as evidence in court. A provision in similar terms to section 9 would render any reference to interception activities inadmissible, whether or not it was authorised. As far as interception of telecommunications is concerned, this would mean that no evidence could be adduced and no question could be asked in cross-examination, which tended to suggest that an offence in relation to the interception of telecommunications had been committed or that a warrant authorising an interception of telecommunications had been issued.

7.38 One respondent to the consultation paper was concerned that the proposal on inadmissibility would preclude the suspect from confronting the basis of an investigation. The suspect might have contended that the intercepted communication had been misinterpreted by the law enforcement agency and, as a result of that mistake, the agency had triggered an elaborate investigation leading to his prosecution. We reiterate that the intercepted material would be used only for intelligence and not as a basis for the decision whether or not to prosecute. Although the suspect would not have an opportunity to correct any mistake made by the agency in compiling the analyses, he would still be able to confront in court the admissible evidence collected on the basis of the intercepted material should a prosecution ensue.

7.39 The Bar Association found it unsatisfactory that lawfully obtained material which may be the only evidence of a crime cannot be used at trial, but instead has to be destroyed. They preferred a regime which would allow the prosecution to decide whether, and to what extent, material obtained pursuant to a warrant is retained and used.

---

[21] The House of Lords explained that this point is of little or no importance in practice because if the regulatory system is working properly the material will have been destroyed long before the trial, and if it is favourable to the accused the prosecution will not have been pursued: *R v Preston* [1993]4 All ER 638 at 672. As section 6 of the 1985 Act requires the destruction of intercepted material once a charge is laid against the accused, the purpose of section 9 can be seen as the protection, not of the fruits of the interception, but of the information as to the manner in which they were authorised and carried out: *op cit*, at 667.

7.40 Other respondents also had reservations on our proposals. The Hong Kong Alliance of Chinese and Expatriates held the view that judges should see as much evidence as was available, particularly when it would be the court which would authorise any intrusion. The Alliance wanted to see a regime in which the prosecution must reveal that intrusive measures had been applied. The Liberal Democratic Federation of Hong Kong was concerned that the work of the law enforcement agencies would be hindered and the deterrent effect weakened if material obtained by interception was inadmissible. They therefore proposed to give the court a discretion to admit such material as evidence depending on its usefulness.

7.41 There were, however, others who agreed with the proposal that intercepted material should be inadmissible. One respondent commented that the legislation should expressly provide that intercepted material should be exempted from pre-trial disclosure to the defence. We agree with this comment in principle. We understand that the law enforcement agencies are satisfied that the adoption of the proposal regarding inadmissibility of intercepted material would not undermine their efforts in fighting crime. Indeed, making intercepted material inadmissible would protect the safety of those who are engaged in covert activities because details of the conduct of an interception would not be made public.

7.42 Material gleaned from an interception is often not specific. Since interception of telecommunications normally lasts for weeks or even months, it is highly likely that personal information which is not relevant to the investigation would be acquired. Much of the information obtained by investigators would probably relate to “innocent” parties who have had contacts with those targeted for interception. If the intercepted material were admissible, this would inevitably result in an invasion of the privacy both of innocent parties and of the target himself. From a privacy point of view, the person whose privacy has been affected by an interception ought to be notified that his right to privacy has been infringed. Problems relating to notification then arise. Who should be notified of an interception? Of what should he be notified? Under what circumstances should he be notified? And when should he be notified? All these problems could be avoided if the privacy of the person affected by an interception could be safeguarded by the destruction of the intercepted material and the rendering of that material inadmissible in court.

7.43 The preceding discussion explains that the principal purpose of interception of telecommunications is the *gathering of intelligence*, and not the collection of evidence for use in prosecutions. It will be recalled that one of the grounds for the

issue of warrants is the "prevention or detection" of serious crime, not the "prosecution" of serious crime. As interception of telecommunications (including telephone tapping) poses a high privacy risk but normally generates material of low probative value, we maintain that material obtained through an interception of telecommunications should be inadmissible in evidence.

7.44 **We recommend that material obtained through an interception of telecommunications carried out pursuant to a warrant shall be inadmissible as evidence regardless of its relevance. For the purposes of this recommendation, "telecommunications" means communications by electromagnetic means. This prohibition should cover not only the fruits of interception but also the manner in which the interception was made.**

7.45 **We recommend that no evidence shall be adduced and no question shall be asked in cross-examination which tends to suggest that an offence in relation to an interception of telecommunications has been committed or that a warrant authorising an interception of telecommunications has been issued.**

* * * * * *

For information
21 February 2006

Legislative Council Panel on Security

Interception of Communications and Covert Surveillance

Response to issues raised by Members at the meeting of 16 February 2006

Introduction

This paper sets out the Administration's response to issues raised by Members at the meeting of the Panel on Security of the Legislative Council (LegCo) on 16 February 2006. The numbering of items follows that set out in the list of issues attached to the letter of the same date from the Clerk to Panel.

Responses to issues raised

Item 1 : To provide statistics on cases of interception of communications and covert surveillance carried out by law enforcement agencies in the past three years.

2. We have further considered the feasibility of compiling the relevant figures in consultation with the law enforcement agencies (LEAs) in light of Members' comments. As explained in the paper presented to the Panel on 16 February 2006, given that the existing system is very different from the proposed one, and that previously there have been no uniform reporting requirements across the LEAs for publication, we consider that it would be impracticable to work out the historical figures post-hoc. Nonetheless, we have asked the LEAs to start keeping the statistics from 20 February 2006. To ensure consistency across the board, the LEAs will keep the statistics on the basis of the proposed legislative regime. We aim to report these statistics to Members after three months.

3. Some Members asked for the number of cases so as to assess at this stage the resource implications for implementing the new regime under the proposed legislation. For the purpose, we will work out an estimate of the number of cases that would require judicial and executive

authorizations had the new legislative regime been in place. We aim to provide Members with this information by the end of the week of 20 February 2006.

Item 2 : To explain the existing regime monitoring the interception of communications and covert surveillance conducted by law enforcement agencies.

4. At the Panel's previous meeting in November 2005, Members discussed our existing regime regulating covert surveillance operations by our law enforcement agencies (LEAs). Currently, the conduct of LEAs in covert surveillance operations is regulated by the Law Enforcement (Covert Surveillance Procedures) Order (the Executive Order) made by the Chief Executive (CE) in July 2005. Under section 17 of the Executive Order, the LEAs have made internal guidelines governing applications for authorizations for covert surveillance, the handling of surveillance product derived from all such operations, the record as well as source protection.

5. To monitor covert surveillance operations, regular reviews by officers senior to the authorizing officers are conducted. The review results are recorded and brought up to the attention of officers at a very senior level. The operations are also subject to housekeeping inspections. The handling of records and materials in relation to the operations concerned is kept under review internally under the regime. In addition, the following safeguards are in place for the handling of materials –

(a) Protection of confidentiality : Details of operations are made known only on a strictly "need to know" basis. All products are properly graded according to the sensitivity of the product and handled accordingly.

(b) Disposal of materials : All products from such operations must be securely destroyed as soon as they are no longer needed after the completion of the operation to protect privacy.

(c) Sensitive information : Special reminders are provided to officers emphasizing that special care must be taken in the handling of sensitive information, in particular, information which may consist of matters subject to legal professional privilege.

Similar monitoring mechanisms and safeguards apply to interception operations.

6. Our legislative proposals seek to stipulate many of the present safeguards in law. In addition, new safeguards such as the oversight by the Commissioner for Interception of Communications and Surveillance (Commissioner) would be included.

Item 3 : To explain whether non-compliance with any code of practice made under the proposed legislation without legal consequences would respect the provisions in Article 30 of the Basic Law (BL30).

7. Under BL30 –

- "The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents"
- "except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences."

For reasons we have explained in previous discussions, we propose that for the current exercise we focus on the second part of BL30 (regulation of operations by LEAs). To fully implement BL30 we will need further work separately on the first part of BL30.

8. While the first part of BL30 requires that the freedom and privacy of communication of Hong Kong residents shall be protected by law, it does not mandate that such protection must be in the form of criminal sanctions. In previous papers which the Law Reform Commission (LRC) has published, the LRC has identified various activities that might infringe upon privacy, and proposed a combination of criminal and civil sanctions against such activities, applicable to all persons in Hong Kong. If after the necessary discussions in our society it is decided to enact legislation on any of such proposed criminal and civil sanctions, such sanctions would apply to LEA officers.

9. Under our proposed regime, we have included very powerful sanctions against non-compliance. A breach under the proposed legislation would be subject to disciplinary proceedings, and this would be stipulated in the code of practice. An officer who deliberately conducts operations without due authorization might also commit the common law offence of misconduct in public office. Any

non-compliance would be subject to the Commissioner's oversight. The Commissioner would also be able to refer any irregularity to the respective head of department, the Chief Executive or the Secretary for Justice. Separately, like everyone in Hong Kong, all public officers have to observe the full range of existing laws.

Item 4 : To provide the definition of interception of communications and to clarify whether the use of a high technology bugging device to pick up conversations at a distance from the premise would be taken as covert surveillance.

10. As explained in the paper presented for discussion at the Panel of Security meeting held on 7 February 2006, interception of communications is commonly understood as the interception of the content of telecommunications or postal articles in the course of their transmission by either a telecommunications system or a postal service. This is the approach used in the 1996 LRC report on interception of communications, the 1997 White Bill, and the Interception of Communications Ordinance (IOCO). We propose to continue to use this approach in our proposed regime, and define the term "interception" along similar lines. Therefore, the surveillance of oral communications (as opposed to telecommunication or postal communications) will be covered under our regime for covert surveillance. We explained in detail our regime for covert surveillance in Annex B of our paper dated 16 February 2006 and the chart tabled at the meeting on 16 February. These papers are enclosed at **Annexes A to C** for easy reference.

11. As can be seen from the enclosed papers, for the use of a listening device to pick up oral communications (and other forms of covert surveillance), the threshold is maximum penalty of 3 years of imprisonment or a fine of $1 million. In other common law jurisdictions, the thresholds for similar operations are –

(a) the United Kingdom (UK) : for intrusive surveillance, offences for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to three years of imprisonment or more, or crimes that involve the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose;

(b) Australia : "relevant offences" include those punishable by imprisonment of 3 years or more, a few other specific offences, and offences prescribed by the regulations; and

(c) the United States (US) : enumerated offences, some of which are punishable by imprisonment for more than one year.

12. If an operation uses a device to pick up conversations (whether in or outside private premises), if this is done from a distance and therefore the conversations cannot be picked up without the aid of the device, the operation would in general be a covert surveillance operation that requires authorization. If there is a participating party, it would require executive authorization; otherwise it would require judicial authorization.

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.

Item 6 : To provide full justifications for not informing a person whose communication sent to or by him has been intercepted by law enforcement agencies or he himself is the subject of covert surveillance operation after such activities have been completed, or otherwise how the person could lodge complaint when he has not been informed of such activities.

15. We have set out our rationale of not informing targets of covert operations of such activities in paragraphs 30 to 31 of the paper presented to the Panel on Security on 16 February 2005. This is in line with the analysis and recommendations of the 1996 LRC report on regulating interception of communications, as well as the practice in the UK and Australia. We attach the relevant extract of the 1996 LRC report at **Annex D** for Members' ease of reference.

16. The European Court of Human Rights has found that the absence of a mandatory notification requirement after a covert surveillance operation is not a violation of the right to privacy. The Court considered that the threat against which surveillance were directed might continue for a long time after the operations. Thus notification to the individuals affected after the operations could compromise the long-term purpose that originally necessitated the surveillance. Such notification might reveal the modus operandi and fields of operation of law enforcement agencies and their agents.

17. A Member asked whether the unavailability of a notification procedure might undermine the effectiveness of the complaints handling system. According to our current thinking, the complaints handling mechanism under the proposed legislation would not impose the onus on the complainant to furnish the Commissioner with "proof" or information to substantiate his claim. Of course, the Commissioner may ask the complainant for information and the complainant may provide the

Commissioner whatever information he considers relevant. More important, however, we plan to empower the Commissioner to obtain relevant information from those who may be able to provide it (who could be any public officer or any other person). As such, the absence of a notification arrangement would not affect the effective operation of the complaints handling system.

Issue 7 : To explain whether the Administration considers that evidence or information known to the prosecution but not the defence would satisfy the principle of equality of arms.

18. The question was asked in the context of the Administration's proposal that products of telecommunication interception operations should not be admitted as evidence. The rationale behind our proposal is set out in paragraphs 35 to 36 of the paper presented to the Panel of Security on 16 February 2006. Our proposal is in line with the analysis and recommendations of the LRC on the evidential use and admissibility of telecommunications intercepts as set out in the 1996 LRC report.

19. We believe that since neither the prosecution nor the defence may adduce any evidence from telecommunications intercepts, there is equality between the two sides in this respect. Given our policy is that intercepts are used for intelligence purpose only, we could not envisage any strong justifications on grounds of fairness of trial for the source of intelligence to be disclosed, which may seriously compromise our future law enforcement capabilities.

20. Nonetheless, we also plan to set out in the legislation specific provisions to allow disclosure to the judge where the disclosure is required in the interests of justice. If the judge considers that the inability to produce the intercept products would result in an unfair trial, he may stay the proceedings. There should therefore be no question of unfairness to the defence.

Item 8 : To provide the overseas legislation on interception of communications and covert surveillance together with their justifications for the provisions to which reference has been made by the Administration in drawing up the legislative proposals.

21. We have taken into account the following legislation in comparable common law jurisdictions –

Australia

Surveillance Devices Act 2004

Australian Security Intelligence Organisation Act 1979

Telecommunications (Interception) Act 1979

Telecommunications (Interception) Amendment Act 2004

Telecommunications (Interception) Amendment (Stored Communications) Act 2004

Canada

Criminal Code: Part VI

Canadian Security Intelligence Service Act

New Zealand

Crimes Act 1961

New Zealand Security Intelligence Service Act 1969

Government Communications Security Bureau Act 2003

United Kingdom

Security Service Act 1989

Intelligence Services Act 1994

Police Act 1997, Part III

Regulation of Investigatory Powers Act 2000

Anti-terrorism, Crime and Security Act 2001

US

Foreign Intelligence Surveillance Act of 1978

Federal Wiretap Act

Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the PATRIOT Act)

22. Our proposals have been worked out after considering this full range of legislation.

Security Bureau
February 2006

For information
7 February 2006

Legislative Council Panel on Security

Proposed Legislative Framework on Interception of Communications and Covert Surveillance

Purpose

This paper sets out proposals for new legislation regulating the conduct of interception of communications and covert surveillance by law enforcement agencies (LEAs).

Background

2. Interception of communications and covert surveillance are two related types of operations. Interception of communications is commonly understood as the interception of the content of telecommunications or postal articles in the course of their transmission by either telecommunications or postal service. Covert surveillance, on the other hand, commonly refers to systematic surveillance undertaken covertly, in situations where the person subject to surveillance is entitled to a reasonable expectation of privacy.

3. These covert investigation tools were a subject of discussions in society and in the former Legislative Council (LegCo) in the 1990's, arising from public concerns on their implications on privacy. In 1996, the Law Reform Commission (LRC) published a consultation paper on interception of communications and covert surveillance. Subsequently it published its report with recommendations for new legislation on interception of communications.

4. In response to the LRC report on **interception of communications**, the Administration published a Consultation Paper with a White Bill annexed in early 1997 incorporating many of the key recommendations of the LRC for consultation. In parallel, LegCo considered a private member's bill and enacted the Interception of Communications Ordinance (IOCO), whose commencement was withheld by the Chief Executive in Council in July 1997 due to its shortcomings. Since then the Administration has been conducting a comprehensive review on the subject of interception of communications. At the meeting of the LegCo Panel on Security on 10 June 2004, the Secretary for Security said that the Administration would

strive to complete the review and revert to the Panel within the 2004-05 legislative session. Developments since (please see paragraphs 5 and 6 below) have made it logical for us to consider the subject together with covert surveillance.

5. On **covert surveillance**, the LRC explained in 1996, when publishing its report on interception of communications, that it had focused on the issue of interception of communications first, and deferred the study of surveillance. It said that the Privacy Sub-committee of the LRC would continue to discuss the issue of surveillance after publication of the report on interception of communications. We understand that the LRC is currently studying the subject. The private member's bill discussed by the then LegCo in 1997 originally covered oral communications (in addition to telecommunications and postal communications), which would be relevant to covert surveillance. At the Committee Stage of scrutinizing the passage of the bill after Second Reading, the bill was amended to exclude oral communications, and as a result the IOCO covers only telecommunications and postal interception.

6. In April 2005, in the Li Man-tak case the District Court judge expressed the view that the covert surveillance operation in the case had been carried out unlawfully, although he eventually allowed the evidence so obtained to be admitted as evidence in the case. In view of the public concerns with such operations that had been expressed following the judge's ruling in that case, in August 2005 the Chief Executive made the Law Enforcement (Covert Surveillance Procedures) Order, and the Administration announced at the same time its intention to regulate covert surveillance operations by means of legislation. At the meeting of the LegCo Panel on Security on 4 October 2005, the Secretary for Security said that proposals for such legislation would be presented to LegCo as soon as possible within the first half of the 2005/06 legislative session.

7. In considering proposals for legislation on interception of communications and covert surveillance, we have taken into account :

- the 1996 LRC consultation paper on regulating surveillance and interception of communications;
- the 1996 LRC report on interception of communications;
- the 1997 White Bill and comments received in response to the White Bill;
- the IOCO;
- comparable legislation of other common law jurisdictions; and
- views expressed on the subject by interested parties, particularly those in exchanges that we have conducted in recent months.

The proposals put forward in this paper, so far as they relate to interception of communications are broadly in line with those in the 1996 LRC report on interception of communications and the 1997 White Bill, with modifications

including those aimed at increasing safeguards in the system. A table comparing the key elements of our proposed system and those in the 1996 LRC report, the IOCO, and the White Bill is at **Annex**.

Proposals for legislation

8. We propose that the new legislation should cover both interception of communications and covert surveillance. In approaching the two subjects, we have taken account of the following –

(a) the need for these investigative techniques to be conducted covertly in the interests of law and order and public security;

(b) the need for adequate safeguards for privacy and against abuse; and

(c) the public's expectation that new legislation regulating the use of these covert investigative techniques should be put in place as early as possible, providing for a proper balance between (a) and (b) above and a statutory basis for such investigative operations.

9. By their nature, interception of communications and covert surveillance operations have to be confidential. There is, therefore, necessarily a limit to the extent to which they may be openly discussed and publicly monitored. Nonetheless, we fully recognize the need to ensure the proper implementation of a regime whilst protecting the privacy of individuals against unwarranted intrusion. In line with international trends, we propose to introduce safeguards at different stages of such operations.

10. The main features of our legislative proposals are set out below.

Non-government parties

11. Article 30 of the Basic Law (BL30) provides that –

> *"The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communications in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences."*

It may therefore be argued that legislative proposals should provide for protection of privacy of communication not only from actions by government parties but also

from actions by non-government parties.

12. The Administration accepts that there should be suitable protection against the infringement of the privacy of communications by both government and **non-government parties**. However, many interlocutors whom we have consulted have advised that given the desirability of new legislation being in place as soon as possible to regulate LEAs' conduct in this area, there is a case for dealing with government parties first and deferring non-government parties to a separate, later exercise.

13. We agree with this advice and therefore propose that we limit the current exercise and our new legislation, to cover Government parties only. It is relevant that the existing law has a number of remedies to deal with the infringement of privacy in general. For example, the collection of personal data is regulated under the Personal Data (Privacy) Ordinance (Cap. 486). The LRC has also published various reports on such related subjects as civil liability for invasion of privacy, which are being considered by the Administration. In addition, the LRC is looking into the subject of covert surveillance. The Administration will study the LRC's further recommendations carefully before considering how best to deal with the infringement of the privacy of communications by other parties.

Authorization

14. For both interception of communications and covert surveillance, we propose that authorization should only be given for the **purposes** of preventing or detecting serious crime (i.e. offences punishable with a maximum imprisonment of not less than 3 years or a fine of not less than $1,000,000 for covert surveillance, or offences punishable with a maximum imprisonment of not less than 7 years for interception of communications) or the protection of public security.

15. Even when the specified purposes apply, authorization should only be given where the **tests of proportionality and hence necessity** are met, taking into account the gravity and immediacy of the case and whether the purpose sought can reasonably be furthered by other less intrusive means. Thus applications for authorization would have to set out such information as the likely intrusion into the privacy of people other than the target and the likely benefit from the proposed operation. The applications would also have to address the possibility of the operation covering any information that may be subject to legal professional privilege.

16. We propose that authorizations granted should be for a **duration** of no longer than three months beginning with the time when it takes effect, should not be backdated, and should be renewable for periods of not exceeding 3 months each

time, subject to similar criteria as for new applications.

17. We propose that it should be possible for an application for authorization or renewal to be made orally if it is not reasonably practicable for the application to be considered in accordance with the normal procedure. Such an application should be followed by a written record within 48 hours of the oral application and the authorizing authority may confirm or revoke the oral approval given. Special provisions would also be made for dealing with very urgent cases, with durations of authorization limited to 48 hours. In both **oral and very urgent application cases**, should the applications be subsequently revoked, the information gathered, to the extent that it could not have been obtained without the authorization, may be ordered to be destroyed immediately.

18. As for the **authorization authority**, we propose that all interception of communications should be authorised by judges. As for covert surveillance, there is a wide spectrum of such operations with varying degrees of intrusiveness. As in many other jurisdictions, it is necessary to balance the need to protect law and order and public security on the one hand, and the need for safeguarding the privacy of individuals on the other. More stringent conditions and safeguards should apply to more intrusive activities.

19. We therefore propose a two-tier authorization system for covert surveillance, under which authorization for "more intrusive" operations would be made by judges, and "less intrusive" operations by designated authorizing officers within LEAs. Surveillance that does not infringe on the reasonably expected privacy of individuals would not require authorization.

20. Whether a covert surveillance operation is "more intrusive" or "less intrusive" depends mainly on two criteria : whether surveillance devices are used and whether the surveillance is carried out by a party participating in the relevant communications. In general, operations involving the use of devices are considered more intrusive. On the other hand, when the use of devices involves a party participating in the relevant communications, the operation is considered less intrusive because that party's presence is known to the other parties and that party may in any case relate the discussion to others afterwards.

21. The authority for authorizing all interception of communications and the more intrusive covert surveillance operations would be vested in one of a panel of judges. Members of the panel would be appointed by the Chief Executive (CE) based on the recommendations of the Chief Justice (CJ). The panel would consist of three to six judges at the level of the Court of First Instance of the High Court. To ensure consistency and to facilitate the building up of expertise, panel members would have a tenure of three years and could be reappointed.

22. For less intrusive covert surveillance, authorization should be given by a senior officer not below a rank equivalent to that of senior superintendent of police, to be designated by the head of the respective LEA.

23. Furthermore, we propose that applications for authorization of these covert operations should only be made by officers of specified departments. These would initially be the Police, the Independent Commission Against Corruption, Customs and Excise Department and Immigration Department. Moreover, applications to the judge (in the case of interception of communications and more intrusive covert surveillance) should only be made after clearance by a directorate officer of the LEA concerned.

Independent oversight authority and complaints handling

24. We propose to establish an **independent oversight authority** to keep under **review LEAs' compliance** with the provisions of the legislation and any code of practice (see para. 31 below). There would also be an **independent complaints handling mechanism** for receiving and investigating complaints against unlawful interception of communications or covert surveillance and awarding compensation. While there may be arguments for separate authorities to perform the oversight and complaints handling functions, our thinking is that the oversight authority could also assume the complaints handling function. The authority, entitled the "Commissioner on Interception of Communications and Surveillance" ("the Commissioner"), is proposed to be a sitting or retired judge not below the level of the Court of First Instance of the High Court, to be appointed by CE. Again CE would consult CJ for recommendations. The term of appointment is proposed to be three years and renewable.

25. We envisage that the Commissioner would conduct sampling audits in carrying out his review function. He would examine compliance and propriety in respect of the information supplied in an application for authorization, the execution of the authorization and the implementation and observance of various safeguards to protect the operation and information gathered. On detecting any irregularities in the course of his review, the Commissioner would be able to bring the matter to the attention of the head of the LEA concerned and request corresponding action to be taken. The head of the LEA would have to report to the Commissioner what action he has decided to take and the reasons. Where he considers it necessary, the Commissioner would also be able to refer such cases to CE or the Secretary for Justice (where, for example, criminal proceedings may be required).

26. The Commissioner, in performing his functions, should have access to any relevant official document. Public officers concerned would be required by

law to support and cooperate with the Commissioner in the performance of his statutory functions. LEAs would also be required to report to the Commissioner all instances of non-compliance with the legislation, terms of authorization or code of practice.

27. The Commissioner would be required to submit **annual reports** to CE on his work, and CE would cause the reports to be tabled in the Legislative Council. The annual report should include information covering interception of communications and covert surveillance respectively, such as the number and duration of authorizations / renewals granted / denied, major categories of offences involved, etc.

28. As far as the complaint mechanism is concerned, a person who believes that any communication sent to or by him has been intercepted by the LEAs, or that he himself is the subject of any covert surveillance operation by the LEAs, would be able to apply for an examination under the mechanism. The complaints authority would consider the complaint by applying the test applicable in a judicial review. If the complaints authority concludes, after examination of the case, that an interception of communications or covert surveillance operation has been carried out by an LEA on the applicant, but was not duly authorized under the legislation where it should have been, the authority may find the case in the applicant's favour. The authority would also be empowered to order the payment of compensation to the applicant. Should the complaints authority detect any irregularities in the course of handling a complaint, the authority may bring the case to the attention of the head of the LEA concerned, as well as the CE or the Secretary for Justice where appropriate.

Regular internal reviews

29. In addition to reviews to be conducted by the Commissioner, the head of LEA concerned would be required to make arrangements to keep under regular review the compliance of officers of the department with authorizations given under the legislation. Moreover, arrangements would be made for officers at a rank higher than those held by the authorizing officers of the department to keep under regular review the exercise and performance by the authorizing officers of the powers and duties conferred or imposed on them by the legislation in respect of less intrusive covert surveillance operations.

Discontinuation of operations

30. Where, before an authorization made ceases to be in force, the officer in charge of the operation is satisfied that the required conditions for obtaining the authorization are no longer satisfied or the purpose for which the authorization

was granted has been achieved, he would be required to cease the operation as soon as practicable, and notify the relevant authorizing authority of the discontinuation of the operation. The authorizing authority would then revoke the authorization.

Code of practice

31. A code of practice for the purpose of providing guidance to law enforcement officers would be prepared under the legislation. We propose that the code be made by the Secretary for Security. The Commissioner may recommend amendments to the code. Any breach of the code of practice would need to be reported to the Commissioner.

Handling and destruction of materials

32. The legislation would require arrangements to be made to ensure that materials obtained by interception of communications and covert surveillance are properly handled and protected. These include keeping the number of persons who have access to the products of interception and surveillance and their disclosure to a minimum, and requiring that such products and any copies made are destroyed or otherwise disposed of as soon as their retention is no longer necessary.

Evidential use

33. We have for a long time adopted the policy of not using telecommunications intercepts as evidence in legal proceedings in order to, among other things, protect privacy. At the same time, intercepts are destroyed within a short time. This ensures an equality of arms between the prosecution and the defence as neither side may use intercepts as evidence. In addition, it minimizes the intrusion into the privacy of innocent third parties through keeping the records which will be subject to disclosure during legal proceedings.

34. On the other hand, covert surveillance products are used as evidence in criminal trials from time to time. As covert surveillance is usually more event and target specific, the impact on innocent third parties and hence privacy concerns are less.

35. We propose that the current policy and practice in respect of evidential use above should be codified in law. The legislation should, therefore, expressly disallow all telecommunications intercepts from evidential use in proceedings. As a corollary, such materials would not be made available to any party in any

proceedings, and questions that may tend to suggest the occurrence of telecommunications interception should also be prohibited from being asked in such proceedings.

Consequential amendments

36. The existing provisions governing interception of postal communications, namely section 13 of the Post Office Ordinance, would be repealed, while the provision governing interception of telecommunications under section 33 of the Telecommunications Ordinance would be retained and suitably amended to cater for the operations of, for example, the Office of the Telecommunications Authority in detecting unlicensed service operators. The Interception of Communications Ordinance would be repealed.

Security Bureau
February 2006

Annex

Comparison of the Administration's Proposals on Interception of Communications and Covert Surveillance with the Proposed Regulatory Regime under the 1996 LRC Report, 1997 White Bill and the Interception of Communications Ordinance (IOCO)

	Current Proposals	1996 LRC Report	White Bill	IOCO
Coverage	- Covert surveillance - Interception of telecommunications - Interception of postal articles	- Interception of telecommunications - Interception of postal article	- Interception of telecommunications (*excluding* messages carried by computer network) - Interception of postal articles	- Interception of telecommunications - Interception of postal article
Applicability	Government parties only[1]	Both government and non-government parties	Both government and non-government parties	Both government and non-government parties
Grounds for authorization	Preventing or detecting serious crime[2] or protecting public security.	Prevention or detection of serious crime[2] or safeguarding of public security in respect of Hong Kong	Prevention/investigation/detection of serious crime[2], or for the security of Hong Kong	Prevention or detection of serious crime[2], or in the interest of security of Hong Kong
Authorization Authority	For interception and more intrusive covert surveillance : 3-6 designated panel judges of the Court of First Instance of the High Court For less intrusive covert surveillance : Senior officers (equivalent in rank to senior superintendent or above) of specified law enforcement departments[3]	For interception: Judges of the Court of First Instance of the High Court	For interception: Not more than 3 designated judges of the Court of First Instance of the High Court	For interception: Judges of the Court of First Instance of the High Court

1 Without prejudice to existing legislative provisions under the Telecommunications Ordinance (Cap 106) on willful interception (sections 24 and 27) or unauthorized opening of postal articles under the Post Office Ordinance (Cap 98) (sections 28 and 29).

2 For interception of communications , serious crime refers to offences punishable with a maximum imprisonment of not less than 7 years in the contexts of our proposals, the White Bill and IOCO. On the other hand, the 1996 LRC Report recommends including offences punishable with a certain maximum imprisonment, to be determined by the Administration. Regarding covert surveillance, serious crime in our proposals refers to offences punishable with a maximum imprisonment of not less than 3 years or a fine of not less than $1,000,000.

3 The specified departments are the Police, Independent Commission Against Corruption, Immigration Department and Customs and Excise Department.

	Current Proposals	1996 LRC Report	White Bill	IOCO
Who may apply for authorizations	For interception and more intrusive covert surveillance : Any officers of specified departments[3] with prior approval by directorate officers For less intrusive covert surveillance : Any officer of specified departments[3]	For interception: Senior officers to be determined by the Administration	For interception: Directorate officers to be authorized by the Chief Executive	For interception: Designated group of officers of specified departments[4]
Maximum duration of authorization	3 months. Renewals allowed	90 days. Renewals allowed	6 months. Renewals allowed	90 days. Only one renewal allowed
Urgent cases	For interception and more intrusive covert surveillance: Approved by Head of Department, followed by written application to a panel judge within 48 hours. Destruction of material if authorization subsequently revoked	For interception : Approved by designated directorate officer, followed by written application to the court within 48 hours. Destruction of material if authorization subsequently rejected	For interception : Approved by an authorized directorate officer, followed by written application to designated judges in 2 working days. Destruction of material if authorization subsequently rejected	For interception : Approved by Head of Department, to be followed by written application to the court within 48 hours from beginning of interception. Destruction of material if authorization subsequently rejected
Evidential use	For telecommunications interception: No evidence shall be adduced and no question shall be asked in court proceedings which tends to suggest an authorized interception has taken place For postal interception and covert surveillance: Usual evidential rules apply	For telecommunications interception: No evidence shall be adduced and no question shall be asked in court proceedings which tends to suggest an authorized or unauthorized interception For postal interception : Usual evidential rules apply	For both telecommunications and postal interception: No evidence shall be adduced and no question shall be asked in court/tribunal proceedings which tends to suggest that an authorized or unauthorized interception	For interception : Evidential use allowed. Prosecution needs to prove beyond reasonable doubt that the material was obtained in accordance with the Ordinance if challenged

[4] Under IOCO, the specified departments are the Police, Independent Commission Against Corruption, Immigration Department, Customs and Excise Department and the Correctional Services Department.

	Current Proposals	1996 LRC Report	White Bill	IOCO
Oversight	Yes – serving or retired judge at the Court of First Instance level of the High Court or above to serve as oversight authority. To review compliance with legislative requirements and handle complaints	Yes – sitting or former Justice of Appeal to serve as supervisory authority. To review compliance with legislative requirements and handle complaints	Yes – Justice of Appeal to serve as supervisory authority. To review compliance with legislative requirements and handle complaints	No oversight mechanism
Reporting to Legislative Council (LegCo)	Annual reports by oversight authority to the Chief Executive (CE) to be tabled at LegCo	Annual reports by supervisory authority to LegCo	Annual reports by supervisory authority to CE to be tabled at LegCo	No annual reports to LegCo. LegCo may require the Secretary for Security to provide specified information from time to time
Remedies	Oversight authority may order payment of compensation to complainants Oversight authority may refer irregularities to CE, the Secretary for Justice (SJ) or Head of Department as appropriate	Revocation of authorization under specified circumstances Supervisory authority may order compensation to complainants Supervisory authority may refer case to SJ (to consider prosecution)	Quashing of authorization Supervisory authority may order compensation to complainant	Court may grant relief by making an order (a) declaring interception or disclosure unlawful, (b) that damages be paid to the aggrieved person, or (c) in the nature of an injunction
Other safeguards	Detailed requirements on record keeping, disclosure, handling and destruction of materials Regular internal reviews by departments Code of practice for law enforcement officers to be issued by the Secretary for Security. It will be publicly available	Requirements on record keeping, disclosure, handling and destruction of materials	Requirements on record keeping, disclosure, handling and destruction of materials	Requirements on record keeping, disclosure, handling and destruction of materials Where no charge is laid against the target within 90 days of the termination of a court order, the court would notify the person that his communications have been intercepted

Security Bureau

February 2006

Annex B

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

<u>Definition of covert surveillance</u>

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).

Annex C

Statutory Requirements for Approval of Covert Surveillance
Comparison of the Administration's Proposals and the Australian Regime [Note 1]

	Listening / Data Surveillance		Optical Surveillance		Tracking	
	Administration's Proposals	**Australia**	**Administration's Proposals**	**Australia**	**Administration's Proposals**	**Australia**
(1) Participant monitoring [Note 2]	Executive	No requirement	Executive	No requirement	Executive	Executive
(2) No participant monitoring and –						
(a) Not involving entry onto premises or interference with the interior of any conveyance or object without permission [Note 3]	Judicial	Judicial	Executive	No requirement	Executive	Executive
(b) Involving entry onto premises or interference with the interior of any conveyance or object without permission [Note 3]	Judicial	Judicial	Judicial	Judicial	Judicial	Judicial

Note 1 : The Australian regime is based on their Surveillance Devices Act 2004.
Note 2 : Assuming that entry onto premises or interference with conveyance or objects without permission is not involved.
Note 3 : In the case of Australia, the interference with object is not a relevant factor for tracking devices, and no distinction is drawn between the interior and exterior of a conveyance or object in considering whether a warrant is required for the use of an optical surveillance device.

Annex D

Relevant Extracts from the 1996 LRC report on interception on communications : Notification

Notification following termination of interception

The notification requirement

7.70 A requirement that the object of interception be notified of the fact that he had been subject to interception once it is terminated is a feature of some but not all laws. In the United States, the Wiretap Act requires that "the persons named in the order or application, and such other parties to intercepted communications as the judge may determine" be notified of the period of interception and such portions of the intercepted communications as the judge may determine.[18] The Canadian Criminal Code also provides that the person who was the object of an authorised interception be notified of that fact. The notice, however, need not include the contents or details of the authorisation.[19] In Germany, "[m]easures of restriction shall be notified to the person concerned after they are discontinued".[20]

7.71 Merely to inform an individual of the fact that he has been the object of interception would serve little purpose. More helpful and informative would be to notify the former target of the sorts of matters covered by the United States provision, including, where appropriate, providing portions of the intercepted communications themselves. We understand that under current Hong Kong practice often only key points from the intercepted communications will be abstracted and retained.

The basis of notification requirement

7.72 The basis of a notification requirement is two-fold. First, it marks the seriousness of the earlier intrusion into privacy. The requirement would introduce an important element of accountability and should deter the authorities from intercepting unnecessarily.

---

18 Section 2518(8)(d).

19 Section 196.

20 German Act on Restriction of Privacy of Mail, Posts and Telecommunications 1989, section 5(5). Indeed one aspect of the German law which was challenged in *Klass* is that there was no requirement that the object of interception be *invariably* notified upon its cessation. The European Court held that this was not inherently incompatible with the privacy provision of the European Convention, provided that the person affected be informed as soon as this could be done without jeopardising the purposes of the interception.

7.73 Secondly, the individual should be able to challenge the grounds on which the intrusion was allowed. Denying the target information that he has been the object of interception will limit the efficacy of the mechanisms enhancing accountability, such as review procedures and the provision of compensation awarded for wrongdoing. We note that the United Kingdom Act lacks a notification requirement and, although compensation is provided for, no claim to date has been successful.

7.74 We think that the public has a right to be told the extent to which intrusions are occurring, although this would partly be addressed by the public reporting requirements to be recommended by us in the next chapter. The adoption of a notification requirement would diminish the need for mechanisms at the stage when the warrant is approved, such as the participation of a third party in the *ex parte* proceedings to represent the interests of the target.[21] There are, however, practical problems in implementing this requirement.

Practical problems of notification

(a) The conflict between notification and the purposes of interception

7.75 A notification requirement would have to be made subject to a proviso ensuring that the operational effectiveness of law enforcement agencies would not be diminished. The requirement would have to be couched in terms that, following the termination of interception, the targets and, perhaps, those innocent parties affected by the interception, should be notified unless this would "prejudice" the purposes of the original intrusion. There would also need to be provision for postponement of the notification on the same grounds.

7.76 "Prejudice", in relation to the target, could be defined to cover the situation where the target is likely to be the object of surveillance or interception in the future and notification is likely to make such surveillance or interception more difficult. This approach would preclude notification of recidivist offenders, or those where there is a reasonable prospect that the investigation may be reopened in the future.

7.77 In the case of notification of "innocent" persons, the most obvious ground on which notification would be denied is if they could be expected to alert the target. Another possibility is that the authorities may wish to tap the innocent person in order to further tap the target again and alerting the innocent person may make this more difficult.

---

[21] E.g. the participation of a "friend of the court".

7.78 The United Kingdom approach is that interception is necessarily clandestine and merely divulging that it has occurred would diminish the value of interception.[22] This obviously runs counter to any requirement of notification.

(b) Prolonged retention of intercepted material

7.79 If part of a notification requirement is to be that details of the fruits of an interception are to be disclosed following the termination of the interception, this necessarily implies that those materials must be retained. This has its own privacy risks.

(c) Resource implications

7.80 If the notification requirement is to be applied meaningfully, it will require the relevant authority to make an informed decision as to whether notification should be effected, applying criteria along the lines described above. Consideration would need to be given to the extent of information to be given to the target under a notification requirement. This raises potentially complex issues and would require the relevant authority to be well briefed on a case by case basis, applying the prejudice test outlined above. The resource implications are obvious. We recommend below that decisions impinging on interceptions should be capable of review. If decisions regarding notification are similarly to be reviewed, the resource implications will be even greater.

The need for notification

7.81 We have recommended that material obtained through interception of telecommunications shall be destroyed immediately after the interceptions have fulfilled the purpose. Destruction of the intercepted material prior to notification would largely destroy the basis of the notification mechanism.[23]

7.82 We have also recommended that material obtained through an interception of telecommunications shall be inadmissible in evidence. If intercepted material were destroyed and inadmissible in court, the risk of dissemination, and hence the riskto privacy, could be reduced to the minimum. There is therefore less need for a notification requirement in Hong Kong than in other jurisdictions where intercepted material may be produced at the trial.

---

22 *R v Preston* [1993] 4 All ER 638 at 648. It is a case on the interception of telephone communications.

23 We recognise that “destruction” is not an absolute concept in the digital age.

7.83 We note that the practice in the United States and Canada is only to notify the public of the fact of interception. It is presumably due to this that those jurisdictions do not appear to have encountered the difficulties we envisage may result from a more extensive notification requirement. We think that a restricted notification requirement along the lines of that in the United States and Canada is of little benefit. Finally, we believe that the accountability aspect is more directly addressed by the warrant system and the public reporting requirement. We have therefore concluded that a person whose telecommunications have been intercepted need not be notified of the interception.

7.84 As regards material obtained by an interception of communications transmitted other than by telecommunication (for example, letters and facsimile copies), although they will not be subject to a destruction requirement and will continue to be admissible in court, we do not think that any privacy problems arise. If the material was adduced in evidence, the suspect would have a right to challenge it in court; and if the material was not required or no longer required for any criminal proceedings, it should have been returned to the addressee or the sender, as the case may be, unless this would prejudice current or future investigation. Further, where one of the parties to the communication is aggrieved by the interception, he may ask for a review under the procedures recommended in Chapter 8 below. It is therefore not necessary for the persons communicating other than by telecommunication to be notified of the fact that his communications had been intercepted or interfered with.

7.85 In conclusion, it is not necessary to provide for a requirement that the object of an interception of communications be notified of the fact that he had been subject to interception. In coming to this conclusion, our main concerns are that such a scheme would have considerable resource and privacy implications, without a clear concomitant benefit. The only exception to this conclusion is where a warrant has been set aside by a judge or the supervisory authority concludes that a warrant had been improperly issued or complied with. We shall explain this in detail in Chapter 8 below.

* * * * * *

For information
2 March 2006

Legislative Council Panel on Security
Interception of Communications and Covert Surveillance

Response to issues raised by Members at the meeting of 21 February 2006

Introduction

This paper sets out the Administration's response to issues raised by Members at the meeting of the Panel on Security of the Legislative Council (LegCo) on 21 February 2006. The numbering of items follows that set out in the list of issues attached to the letter of the 24 February 2006 from the Clerk to Panel.

Responses to issues raised

Item 1 : To advise whether there will be any provisions prohibiting the use of information obtained by interception of communications or covert surveillance for other purposes and how compliance with such provisions will be monitored.

2. The Interception of Communications and Surveillance Bill (the Bill) sets out in detail the safeguards for the disclosure and retention of interception or covert surveillance products (protected products). Under the Bill, disclosure of protected products or their copies is required to be kept to the minimum that is necessary for the relevant purpose of the prescribed authorization. Something is necessary for the relevant purpose of the prescribed authorization only if it continues to be, or is likely to become, necessary for the purpose sought to be furthered by carrying out the operation concerned or (except in the case of telecommunications interception) if it is necessary for the purposes of any pending or anticipated civil or criminal proceedings.

3. Within each law enforcement agencies (LEAs), arrangements would be made to minimize the extent to which protected products are disclosed or copied, or are subject to unauthorized or accidental access, processing, erasure or other use, and to ensure their proper destruction for the protection of privacy. This would help avoid misuse of the products of the operations in question.

4. The proposed regime would have a stringent review system, by both the Commissioner on Interception of Communications and Surveillance (the Commissioner) as well as internally, to ensure compliance with the new legislation and any code of practice that may be made under the legislation. Externally, reviews would be conducted by the Commissioner, who would be a sitting or former judge at or above the level of the Court of First Instance. He would examine compliance and propriety in respect of the information supplied in an application for authorization, the execution of the authorization and the implementation and observance of various safeguards to protect the operation and information gathered. The Commissioner would also be able to refer any irregularity to the respective head of department, the Chief Executive or the Secretary for Justice. Internally, the head of the LEAs concerned would be required to make arrangements to keep under regular review the compliance by officers of the department with the relevant requirements, including the provisions of the legislation, code of practice and the requirements under the authorizations given.

5. Moreover, as explained in our response to questions raised by Members at the Panel meeting on 16 February 2006, under our proposed regime, there will be powerful sanctions against non-compliance. An officer who breaches the proposed legislation would be subject to disciplinary proceedings. An officer who deliberately conducts operations without due authorization may also commit the common law offence of misconduct in public office.

6. In their totality, the measures set out above provide a strong system ensuring compliance of LEA officers with the strict requirements regarding the disclosure and retention of protected products from interception or covert surveillance.

Item 2 : To advise whether there are any guidelines prohibiting suspects or witnesses from recording conversations with law enforcement officers, without the knowledge of the latter, during the taking of statements.

7. The Bill only regulates the conduct of public officers and people acting on their behalf in carrying out interception and covert surveillance. It would not affect the conduct of other individuals nor create any liability for them in this regard.

8. The Rules and Directions for the Questioning of Suspects and

the Taking of Statements (Rules and Directions), issued by the Secretary for Security, contain guidelines for LEA officers in the taking of statements from suspects in order to protect these suspects' rights. The suspects have the right to request a record of the interview. There is no specific provision in the Rules and Directions prohibiting the use of recording equipment by the suspects, nor are there any other law or guidelines against such acts. However, if the statement taking process occurs whilst a suspect is in custody, the question of recording should not arise because the suspect would not have access to his own recording device. In any case, suspects will be given a copy of all statements taken from them.

Item 3 : To reconsider the suggestion of notifying the targets of interception of communications or covert surveillance operations after such activities have discontinued, and applying to the court for not notifying the targets.

9. As explained in our previous papers, our current proposal of not notifying the targets of operations is in line with the analysis and recommendations of the 1996 LRC report on regulating interception of communications, as well as the practice in the United Kingdom and Australia. This is because threats being targeted by interception of communications or covert surveillance might continue for a long time after the operations. Thus notification to the individuals affected after the operation has ceased could still compromise the long-term purpose that originally necessitated the surveillance. Such notification might reveal the modus operandi and fields of operation of LEAs and their agents. In many cases this may ruin years of hard work and even subject the safety of LEA officers as well as those of the victims or witnesses to unnecessary risks. This would benefit criminal syndicates which are becoming increasingly organized and sophisticated.

10. Even for less sophisticated criminals, convictions are not necessarily the outcomeof every operation. A notification requirement could greatly reduce the chance of successfully conducting the same surveillance operation on the same criminal again.

11. From a privacy point of view, a notification requirement would logically require relevant materials to be kept for the purpose of notification and any subsequent complaints arising. This would result in the need for related materials to be kept, and is contrary to the principle of destruction of such materials as early as possible to protect privacy.

12. As explained in the paper for the Panel's discussion on 21 February 2006, the complaints handling mechanism would not impose the onus on the complainant to furnish the Commissioner with "proof" or information to substantiate his claim. The Commissioner would be empowered to obtain relevant information from those who may be able to provide it (who may be any public officer or any other person). As such, the absence of a notification arrangement would not affect the effective operation of the complaints handling system.

13. It should be emphasized that notification is only one of the safeguards against abuse. With other safeguards in the Bill as explained in our papers for the Panel's discussion on 7, 16 and 21 February, we consider that the present package represents a balanced approach in protecting the privacy of the individuals as well as ensuring the effectiveness of LEAs in carrying out their duties to protect the public. The jurisprudence of the European Court of Human Rights also supports the view that the absence of a mandatory notification requirement after a covert surveillance operation is not necessarily a violation of the right to privacy, and that safeguards should be seen in their totality. We believe that, viewed as a whole, the various safeguards included in our proposals are adequate and compare favourably with that in many common law jurisdictions.

14. We attach at **Annex** the relevant extracts of our previous responses on the subject for Members' ease of reference.

Item 4: To explain the consideration factors or criteria adopted for proposing the appointment of a panel of judges by the Chief Executive for authorizing interception of communications and the more intrusive covert surveillance operations, and the differences between the aforementioned proposed framework and the franework for authorizing the issuance of search warrants by judges in terms of the role of judges, the procedures involved and the appeal or judicial review of the decisions of judges.

Item 5 : To explain why the Administration considers it appropriate for the Chief Executive to appoint a panel of judges for authorizing interception of communications and the more intrusive covert surveillance, and to clarify the functions of the panel judges, whether the decisions of the panel judges are subject to judicial review and whether the panel judges are subject to any rules or procedures of the court.

15. The powers of CE under Article 48 of the Basic Law (BL48) include, inter alia, the power to appoint and remove judges of the courts at all levels. BL 88 further provides that the judges of the court of the HKSAR shall be appointed by CE on the recommendation of the Judicial Officers Recommendation Commission. That function reflects the role of CE under the Basic Law as head of the Hong Kong Special Administrative Region. Our current proposal for CE to appoint a panel of judges for authorizing interception of communications and the more intrusive covert surveillance is in line with that role and more generally the principle of executive-led government. There are many other statutory offices to which judges may be appointed, and CE is almost invariably the appointing authority[1]. The fact that they are appointed by CE in no way affects their independence in carrying out their statutory functions.

16. Moreover, as clearly provided for in the Bill, CE will only appoint the panel judges on the recommendation of the Chief Justice (CJ). As previously pointed out, prior to making the appointments, CE would ask CJ for recommendations. In other words, CE would only appoint someone recommended by CJ. The term of appointment would be fixed at three years, and we propose that CE would only revoke an appointment on CJ's recommendation and for good cause. There is no question of CE interfering with the consideration of individual cases or indeed the assignment of judges from within the panel to consider individual cases.

17. As set out in our earlier response to the questions raised by Members at the Panel meeting on 7 February 2006 (discussed at the Panel meeting on 16 February 2006), the proposed appointment arrangement would be comparable with the arrangement elsewhere for the appointment to be made by a senior member of the government. For example, in Australia, a Minister nominates the members of the Administrative Appeals Tribunal to approve interception of communications. In the UK, the Prime Minister appoints the Surveillance Commissioner for approving intrusive surveillance operations after they have been authorized by the executive authorities.

18. As regards the framework of the new regime, the Bill provides that a panel judge when carrying out his functions will act judicially, but

---

[1] Examples include the chairmanship of the following: the Securities and Futures Appeals Tribunal under Cap 571; the Long-term Prisoners Sentences Review Board under Cap 524; the Post Release Supervision Board under Cap 475; the Administrative Appeals Board under Cap 442; the Market Manipulation Tribunal under Cap 571; and a Commission of Inquiry under Cap 86.

not as a court or as a member of a court and that he will have all the powers and immunities of a judge of the High Court[2]. Conceptually this is not an unusual arrangement. For example, a Commissioner appointed under the Commissions of Inquiry Ordinance (Cap 86) will similarly not act as a court, although for all intents and purposes he will act judicially in carrying out his functions. Since a panel judge will not be acting as a court, he may be liable to judicial review in respect of his decisions. The Bill seeks to establish a self-contained statutory regime. In this respect the proceedings will not be generally subject to rights of appeal or other provisions of the High Court Ordinance or High Court Rules. The similarity with the issue of a subpoena or search warrant is only limited, in that the importance of the issues to be dealt with and their sensitivity are considerably different, hence justifying the setting up of the self-contained statutory regime that we have proposed.

Item 6. To consider the suggestion that some highly intrusive covert surveillance activities, for example the use of bugging device to pick up communications, should require a higher threshold as in the case of interception of communications which requires offences to be punishable with a maximum imprisonment of not less than seven years.

19. As set out in our previous responses, interception is considered to be a highly intrusive investigative technique and therefore a high threshold is necessary. On the other hand, there is a wide spectrum of covert surveillance operations with varying degree of intrusiveness. Since surveillance operations can be more specific in terms of location, timing and event, the intrusiveness in terms of collateral intrusion to innocent party could be much lower. It would therefore be reasonable to include a wider spectrum of crimes against which the investigative technique of covert surveillance may be used, **where justified**.

20. In this connection, we would emphasize again that the limitation on the penalties of crime stipulated is only the initial screen and is by no way the only determining factor. In all cases, authorization would only be given if the tests of proportionality and necessity are satisfied. The relevant factors in considering the balancing test, as detailed in the Bill, include the immediacy and gravity of the crime, and the intrusiveness of the operation. Highly intrusive surveillance

---

[2] In the case of *Bruno Grollo v. Michael John Palmer, Commissioner of the Australian Federal Police and Others F.C.95/032*, the Australian Court was of the view that issuing an interception warrant was a non-judicial power and as such held that a non-judicial function could not be conferred on a Judge without his or her consent.

activities could only be justified where the crime concerned is sufficiently serious and where such threat is immediate.

Item 7. To advise on the resource implications on law enforcement agencies of the implementation of the proposed legislation.

21. The proposals to establish an authorization authority and an independent oversight authority together with a complaint mechanism involving the payment of compensation will have financial and staffing implications. The LEAs would also have to deploy resources to put in place the new system within their departments. We are still assessing the resource implications more fully, and will do so in parallel with the discussion of the Bill with LegCo. We will try to meet the additional requirements from existing resources if possible and will seek additional resources where necessary in line with established procedures.

Security Bureau
March 2006

Annex

Interception of Communications and Covert Surveillance
Response to the Issue of Notification of Targets by the Administration

Extract of Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 16 : To advise whether any person whose communication sent to or by him has been intercepted by the law enforcement agencies or he himself is the subject of any covert surveillance operation would be informed of such activities conducted, and if not, the justifications for that.

30. In the 1996 LRC report, the LRC explained why it concluded against notification of targets of interception of communications. In essence, the LRC recognized the conflict between notification and the purposes of interception, which is necessarily clandestine. Notification could affect the operational effectiveness of LEAs. The prolonged retention of intercepted material arising from a notification requirement would have its own privacy risks. In addition, if the notification requirement is to be applied meaningfully, it will require the relevant authority to make an informed decision as to whether notification should be effected and the extent of information to be given to the target on a case by case basis. The resource implications are obvious. Also, destruction of the intercepted material prior to notification would largely destroy the basis of the notification mechanism. In line with the LRC's recommendation that material obtained through an interception of telecommunications shall be inadmissible in evidence, if intercepted material were destroyed and inadmissible in court, the risk of dissemination, and hence the risk to privacy, could be reduced to the minimum. We agree with the LRC's analysis and recommendations.

31. We note that neither the UK nor Australia has a notification arrangement. Given our policy in respect of the handling of telecommunications intercepts (see paragraphs 35 to 36 below), there is all the more reason not to notify the target. In covert surveillance cases where the product of covert surveillance would be able to be introduced into court proceedings, the product could be introduced into evidence or be disclosed as unused material, and the aggrieved person would be able to challenge it in court.

Extract of Information Paper for the meeting of LegCo Panel on Security on 21 February 2006

Item 6 : To provide full justifications for not informing a person whose communication sent to or by him has been intercepted by law enforcement agencies or he himself is the subject of covert surveillance operation after such activities have been completed, or otherwise how the person could lodge complaint when he has not been informed of such activities.

15. We have set out our rationale of not informing targets of covert operations of such activities in paragraphs 30 to 31 of the paper presented to the Panel on Security on 16 February 2005. This is in line with the analysis and recommendations of the 1996 LRC report on regulating interception of communications, as well as the practice in the UK and Australia. We attach the relevant extract of the 1996 LRC report at **Annex D** for Members' ease of reference.

16. The European Court of Human Rights has found that the absence of a mandatory notification requirement after a covert surveillance operation is not a violation of the right to privacy. The Court considered that the threat against which surveillance were directed might continue for a long time after the operations. Thus notification to the individuals affected after the operations could compromise the long-term purpose that originally necessitated the surveillance. Such notification might reveal the modus operandi and fields of operation of law enforcement agencies and their agents.

17. A Member asked whether the unavailability of a notification procedure might undermine the effectiveness of the complaints handling system. According to our current thinking, the complaints handling mechanism under the proposed legislation would not impose the onus on the complainant to furnish the Commissioner with "proof" or information to substantiate his claim. Of course, the Commissioner may ask the complainant for information and the complainant may provide the Commissioner whatever information he considers relevant. More important, however, we plan to empower the Commissioner to obtain relevant information from those who may be able to provide it (who could be any public officer or any other person). As such, the absence of a notification arrangement would not affect the effective operation of the complaints handling system.

Annex D to Information Paper
on 21 February 2006

Relevant Extracts from the 1996 LRC report on interception on communications : Notification

Notification following termination of interception

The notification requirement

7.70 A requirement that the object of interception be notified of the fact that he had been subject to interception once it is terminated is a feature of some but not all laws. In the United States, the Wiretap Act requires that "the persons named in the order or application, and such other parties to intercepted communications as the judge may determine" be notified of the period of interception and such portions of the intercepted communications as the judge may determine.[18] The Canadian Criminal Code also provides that the person who was the object of an authorised interception be notified of that fact. The notice, however, need not include the contents or details of the authorisation.[19] In Germany, "[m]easures of restriction shall be notified to the person concerned after they are discontinued".[20]

7.71 Merely to inform an individual of the fact that he has been the object of interception would serve little purpose. More helpful and informative would be to notify the former target of the sorts of matters covered by the United States provision, including, where appropriate, providing portions of the intercepted communications themselves. We understand that under current Hong Kong practice often only key points from the intercepted communications will be abstracted and retained.

The basis of notification requirement

7.72 The basis of a notification requirement is two-fold. First, it marks the seriousness of the earlier intrusion into privacy. The requirement would introduce an important element of accountability and should deter the authorities from intercepting unnecessarily.

---

18 Section 2518(8)(d).

19 Section 196.

20 German Act on Restriction of Privacy of Mail, Posts and Telecommunications 1989, section 5(5). Indeed one aspect of the German law which was challenged in *Klass* is that there was no requirement that the object of interception be *invariably* notified upon its cessation. The European Court held that this was not inherently incompatible with the privacy provision of the European Convention, provided that the person affected be informed as soon as this could be done without jeopardising the purposes of the interception.

7.73 Secondly, the individual should be able to challenge the grounds on which the intrusion was allowed. Denying the target information that he has been the object of interception will limit the efficacy of the mechanisms enhancing accountability, such as review procedures and the provision of compensation awarded for wrongdoing. We note that the United Kingdom Act lacks a notification requirement and, although compensation is provided for, no claim to date has been successful.

7.74 We think that the public has a right to be told the extent to which intrusions are occurring, although this would partly be addressed by the public reporting requirements to be recommended by us in the next chapter. The adoption of a notification requirement would diminish the need for mechanisms at the stage when the warrant is approved, such as the participation of a third party in the *ex parte* proceedings to represent the interests of the target.[21] There are, however, practical problems in implementing this requirement.

Practical problems of notification

(a) The conflict between notification and the purposes of interception

7.75 A notification requirement would have to be made subject to a proviso ensuring that the operational effectiveness of law enforcement agencies would not be diminished. The requirement would have to be couched in terms that, following the termination of interception, the targets and, perhaps, those innocent parties affected by the interception, should be notified unless this would "prejudice" the purposes of the original intrusion. There would also need to be provision for postponement of the notification on the same grounds.

7.76 "Prejudice", in relation to the target, could be defined to cover the situation where the target is likely to be the object of surveillance or interception in the future and notification is likely to make such surveillance or interception more difficult. This approach would preclude notification of recidivist offenders, or those where there is a reasonable prospect that the investigation may be reopened in the future.

7.77 In the case of notification of "innocent" persons, the most obvious ground on which notification would be denied is if they could be expected to alert the target. Another possibility is that the authorities may wish to tap the innocent person in order to further tap the target again and alerting the innocent person may make this more difficult.

---

[21] E.g. the participation of a "friend of the court".

7.78 The United Kingdom approach is that interception is necessarily clandestine and merely divulging that it has occurred would diminish the value of interception.[22] This obviously runs counter to any requirement of notification.

(b) Prolonged retention of intercepted material

7.79 If part of a notification requirement is to be that details of the fruits of an interception are to be disclosed following the termination of the interception, this necessarily implies that those materials must be retained. This has its own privacy risks.

(c) Resource implications

7.80 If the notification requirement is to be applied meaningfully, it will require the relevant authority to make an informed decision as to whether notification should be effected, applying criteria along the lines described above. Consideration would need to be given to the extent of information to be given to the target under a notification requirement. This raises potentially complex issues and would require the relevant authority to be well briefed on a case by case basis, applying the prejudice test outlined above. The resource implications are obvious. We recommend below that decisions impinging on interceptions should be capable of review. If decisions regarding notification are similarly to be reviewed, the resource implications will be even greater.

The need for notification

7.81 We have recommended that material obtained through interception of telecommunications shall be destroyed immediately after the interceptions have fulfilled the purpose. Destruction of the intercepted material prior to notification would largely destroy the basis of the notification mechanism.[23]

7.82 We have also recommended that material obtained through an interception of telecommunications shall be inadmissible in evidence. If intercepted material were destroyed and inadmissible in court, the risk of dissemination, and hence the riskto privacy, could be reduced to the minimum. There is therefore less need for a notification requirement in Hong Kong than in other jurisdictions where intercepted material may be produced at the trial.

---

22 *R v Preston* [1993] 4 All ER 638 at 648. It is a case on the interception of telephone communications.

23 We recognise that “destruction” is not an absolute concept in the digital age.

7.83 We note that the practice in the United States and Canada is only to notify the public of the fact of interception. It is presumably due to this that those jurisdictions do not appear to have encountered the difficulties we envisage may result from a more extensive notification requirement. We think that a restricted notification requirement along the lines of that in the United States and Canada is of little benefit. Finally, we believe that the accountability aspect is more directly addressed by the warrant system and the public reporting requirement. We have therefore concluded that a person whose telecommunications have been intercepted need not be notified of the interception.

7.84 As regards material obtained by an interception of communications transmitted other than by telecommunication (for example, letters and facsimile copies), although they will not be subject to a destruction requirement and will continue to be admissible in court, we do not think that any privacy problems arise. If the material was adduced in evidence, the suspect would have a right to challenge it in court; and if the material was not required or no longer required for any criminal proceedings, it should have been returned to the addressee or the sender, as the case may be, unless this would prejudice current or future investigation. Further, where one of the parties to the communication is aggrieved by the interception, he may ask for a review under the procedures recommended in Chapter 8 below. It is therefore not necessary for the persons communicating other than by telecommunication to be notified of the fact that his communications had been intercepted or interfered with.

7.85 In conclusion, it is not necessary to provide for a requirement that the object of an interception of communications be notified of the fact that he had been subject to interception. In coming to this conclusion, our main concerns are that such a scheme would have considerable resource and privacy implications, without a clear concomitant benefit. The only exception to this conclusion is where a warrant has been set aside by a judge or the supervisory authority concludes that a warrant had been improperly issued or complied with. We shall explain this in detail in Chapter 8 below.

* * * * * *