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