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.

* * * * * *