For information
16 March 2006 **SB Ref: ICSB 1/06**

Bills Committee on Interception of Communications and Surveillance Bill

Overview

Purpose

This paper gives an overview of the Interception of Communications and Surveillance Bill (the Bill), and provides a summary of the related discussions at the Panel on Security (the Panel).

The Bill

2. The background to the Bill is set out in the Legislative Council Brief dated 1 March 2006. In essence, the Bill provides a new legal basis for interception of communications and covert surveillance operations by the law enforcement agencies (LEAs), replacing the current systems under section 33 of the Telecommunications Ordinance and the Law Enforcement (Covert Surveillance Procedures) Order. Its object is to regulate the conduct of interception of communications and the use of surveillance devices by or on behalf of public officers. The Bill contains six Parts and five Schedules.

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

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

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

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

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

8. Part 6 contains miscellaneous provisions.

Summary of Discussions at Panel on Security

9. The Panel discussed the legislative proposals underlying the Bill at its meetings held on 7, 16 and 21 February and 2 and 7 March respectively. As the Bills Committee may wish to refer to those discussions, we set out below the key points discussed for Members' ease of reference.

(a) Coverage of the Regime

10. We have limited our proposed legislation to government entities, and proposed to leave non-government entities to a future exercise. Our further clarification in response to the Panel's questions in this regard is extracted at **Annex A1**.

(b) Authorization Authorities

11. We propose that a member of a panel of three to six senior judges be appointed by the Chief Executive (CE) on the recommendation of the Chief Justice for the purpose of considering applications for all interceptions and the more intrusive covert surveillance operations. For less intrusive covert surveillance operations, we propose that they be authorized by designated senior officers of an LEA appointed by the head of the department concerned.

12. The Panel has discussed whether the panel of judges should be appointed by CE; whether the term of appointment of these judges can be made more secure; and the implications of these appointment arrangements on the independence of the panel judges. We have explained that the proposed appointment arrangement is entirely appropriate, and that there is no question of the independence of the panel judges being compromised. The relevant extracts of the Administration's response are at **Annex A2**.

13. The Panel has also asked for the justifications for the establishment of a separate panel of judges and how the judges would function. We have explained the need for a self-contained regime given the unique nature of the cases involved and the need to build up expertise. The relevant extract of the Administration's response is at **Annex A3**.

14. The Panel has discussed whether it would be appropriate to subject panel judges to extended checking. The Administration has advised that this is a standard operational arrangement applicable to those with wide access to sensitive information, and will apply to the judges, their support staff, the proposed Commissioner, and his support staff. Please also see paragraph 24 below.

(c) The Authorization Mechanism

15. The Administration proposes that in all cases, the authorization should only be given for the purpose of prevention or detection of serious crime[1] or protection of public security. These are specified in Article 30 of the Basic Law as grounds for the relevant authorities to inspect communication. In addition, the tests of necessity and proportionality would have to be met. Applications should be made in writing to the respective authorization authorities except in special or emergency situations where it is not reasonably practicable for the application to be considered in accordance with the normal procedures, in which case oral or emergency applications could be made. Authorizations should be granted for a duration of no longer than three months except in the case of emergency applications where the authorization would only be valid for a maximum of 48 hours.

16. The Panel has asked how "more intrusive" and "less intrusive" operations would be differentiated and the justifications for a two-tier approach in authorization. The Panel has also discussed the threshold for covert surveillance. We have explained in some detail the distinction between more intrusive and less intrusive covert surveillance, together with a table comparing our proposal in this regard with the practice in Australia. We have also pointed out that the threshold is but an initial screen, and that the other tests set out in the legislation have to be met as well. The relevant extracts of the Administration's response on these various issues are at **Annex A4**.

17. The Panel has also asked questions on the renewal of authorizations and the circumstances under which oral / urgent applications could be made. The relevant extracts of the Administration's response on these issues are at **Annexes A5 and A6**.

---

[1] For interception of communications, serious crime refers to offences punishable with a maximum imprisonment of not less than 7 years. For covert surveillance, serious crime refers to offences punishable with a maximum imprisonment of not less than 3 years or a fine of not less than $1,000,000.

(d) Independent Oversight and Complaints Handling

18. The Bill provides for an independent oversight authority (i.e. the Commissioner) to keep under regular review LEAs' compliance with the requirements of the provisions of the new legislation, the code of practice and any prescribed authorization. The Commissioner would also be responsible for receiving and investigating complaints against unlawful interception or covert surveillance. The Commissioner's annual report would be tabled at LegCo.

19. The Panel has sought clarifications on the operation of the proposed complaints mechanism, in particular whether there should be some form of notification after the operation. We have set out how the Commissioner would generally operate. We have also explained the factors that we have taken into account in coming up with the current proposal, and the problems associated with notification. The relevant extracts of the Administration's response are at **Annex A7**.

20. The Panel has also discussed the desirability of appointing a serving or retired judge as the Commissioner and whether the Commissioner would have sufficient support to carry out his duties. The Administration has explained the rationale for appointing the Commissioner from serving or retired judges, that appointing a single person as a statutory authority is not an unusual arrangement, and that sufficient resources will be provided to the Commissioner for carrying out his duties. The relevant extracts of the Administration's response are at **Annex A8**.

(e) Other Safeguards

21. Apart from the independent oversight cum complaint handling arrangement set out above, the Bill also provides for further safeguards, including the requirements for regular reviews and protection against unauthorized disclosure. Also, it seeks to codify our long-established policy of not using telecommunications intercepts as evidence in court proceedings, but allowing products of covert surveillance to be introduced as evidence.

22. Apart from the issue of notification of targets covered in para. 19 above, the Panel has in this context asked about sanctions for non-compliance and whether the code of practice would be subsidiary legislation. We have explained that LEA officers who fail to comply with the new legislation would be subject to disciplinary action or, depending on the cases, the common law offence of misconduct in public office, in addition to continuing to be subject to the full range of existing law. The code of practice would be published, but would not be subsidiary legislation. The relevant extracts of

the Administration's response are at **Annex A9**.

23. The Panel has asked about safeguards for information obtained from interception of communications and covert surveillance and treatment of information that may be subject to the protection of legal professional privilege. We have explained that there will be requirements for safeguarding the protected products, and that judicial authorization would be required for all covert surveillance that may acquire information subject to legal professional privilege. The relevant extracts of the Administration's response are set out at **Annex A10**.

24. We have also explained to the Panel that in line with our established operational arrangement for safeguarding sensitive information, we will subject the panel judges, the Commissioner, and their respective staff to extended checking. Details that we have provided to the Panel are at **Annex A11**.

25. On evidential use, the Panel has asked if equality of arms would be satisfied if materials obtained by telecommunications are not admissible as evidence. We have explained that there would not be any inequality as neither side might use the material. The relevant extracts of the Administration's response on this point are set out at **Annex A12**.

(f) Resource Implications

26. The Panel has asked about the resource implications of our legislative proposals on the Judiciary and LEAs. We have explained that we would provide the Judiciary with sufficient resources for implementing the proposals, and that any additional resources would be dealt with in accordance with established procedures. The relevant extracts of the Administration's response on this point are set out at **Annex A13**.

27. The Panel has also asked for the current caseload for assessing the likely resource implications on the Judiciary. The Administration has provided to the Panel the number of cases of interception of communications and covert surveillance in the last three months of 2005. Statistics have also started to be kept from 20 February 2006 on the number of cases of such operations for three months. The relevant information provided by the Administration on this issue is set out at **Annex A14**.

Security Bureau
March 2006

Annex A1

Interception of Communications and Covert Surveillance

Coverage of the Regime

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 1 : To clarify whether the protection of public security includes the protection of national security.

2. The question was asked in relation to Article 23 of the Basic Law (BL23). As the Secretary for Security indicated at the meeting of the Panel on Security on 7 February 2006, the present exercise is unrelated to the BL23 exercise. No interception of communications or covert surveillance would be carried out for offences under BL23 that have yet to be created.

3. We have referred to "public security" in our proposals as it is the term used in Article 30 of the Basic Law. As can be seen from the 1996 Law Reform Commission (LRC) Report on interception of communications (the 1996 LRC report), the 1997 White Bill on Interception of Communications and the 1997 Interception of Communications Ordinance (IOCO), the approach generally is to leave the term "public security" undefined so that security cases are considered and justified on their own individual circumstances. All applications must satisfy the tests set out in the law. All interceptions and more intrusive covert surveillance operations would have to be approved by a member of the panel of judges. In addition, all such operations would be subject to oversight by the proposed Commissioner on Interception of Communications and Surveillance (the Commissioner).

Item 2 : To clarify whether Mainland public security authorities and State security organs are within the meaning of non-government parties under the proposed new legislation.

4. During this first stage of the exercise, we seek to authorize and regulate the conduct of our law enforcement agencies (LEAs) and we would in fact be specifying those departments under the law. Non-government entities would not be dealt with at this stage under our current proposals. For similar activities of parties other than those of the Hong Kong Special

Administrative Region Government, they are subject to current laws (statutes and common law) that apply to all persons in Hong Kong (please see paragraph 15 below). They will also be subject to any future laws that may be made in this and other related areas. In this connection, the following studies the LRC has done or is doing may be relevant –

- its 1996 report on interception of communications proposing criminal offences for certain activities by both government and non-government parties;
- its 2004 report on civil liability for invasion of privacy proposing to create civil liabilities for the invasion of privacy;
- its 2004 report on privacy and media intrusion proposing to establish an independent and self-regulating press commission for the protection of privacy, to handle complaints against the press and draw up a Press Privacy Code for the practical guidance of the press; and
- its 2000 report on stalking proposing the creation of a criminal offence for stalking.

These issues may be dealt with separately.

* * * * * *

Annex A2

Interception of Communications and Covert Surveillance

Appointment of Panel of Judges

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 14 : To reconsider whether the panel of judges authorizing interception of communications and the more intrusive covert surveillance operations should be appointed by the Chief Executive.

23. Vesting the approving authority for interception of communications and the more intrusive covert surveillance in a panel of High Court judges would –

- ensure that the cases would be considered by senior judges with considerable judicial experience;
- allow the building up of expertise in dealing with the usually highly sensitive cases;
- facilitate the application of consistent standards in dealing with the cases; and
- facilitate the Judiciary in planning and deploying judicial resources, for example, in the listing of cases.

We have consulted the Judiciary and the Judiciary's position is that the proposal is acceptable.

24. Prior to making the appointments, CE would ask the Chief Justice (CJ) for recommendations. In other words, CE would only appoint someone recommended by CJ. The term of appointment would be fixed at three years, and we propose that CE would only revoke an appointment on CJ's recommendation and for good cause. We have consulted the Judiciary, and the Judiciary's position is that the proposal is acceptable.

25. Judges appointed to the panel will receive no advantages from that appointment. They will continue to be judges and whatever they do while

on the panel will in no way affect their continued eligibility as judges. That they are appointed by CE to the panel therefore would give no positive or negative incentives that might affect their independence when carrying out their duties as judges on the panel.

26. Designating selected judges to deal with different types of case is not uncommon either in Hong Kong or overseas. For example, the Judiciary practises a listing system designating certain judges to handle certain types of case. In the US, applications for foreign electronic surveillance orders may only be made to one of 11 federal judges. The Australian experience also indicates that not all judges are prepared to take up the responsibility.

27. The proposed appointment arrangement takes into account the above considerations; and would be comparable with the arrangement elsewhere for the appointment to be made by a senior member of the government. For example, in Australia, a Minister nominates the members of the Administrative Appeals Tribunal to approve interception of communications. In the UK, the Prime Minister appoints the Surveillance Commissioner for approving intrusive surveillance operations.

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 2 March 2006

Item 4: To explain the consideration factors or criteria adopted for proposing the appointment of a panel of judges by the Chief Executive for authorizing interception of communications and the more intrusive covert surveillance operations, and the differences between the aforementioned proposed framework and the franework for authorizing the issuance of search warrants by judges in terms of the role of judges, the procedures involved and the appeal or judicial review of the decisions of judges.

Item 5 : To explain why the Administration considers it appropriate for the Chief Executive to appoint a panel of judges for authorizing interception of communications and the more intrusive covert surveillance, and to clarify the functions of the panel judges, whether the decisions of the panel judges are subject to judicial review and whether the panel judges are subject to any rules or procedures of the court.

15. The powers of CE under Article 48 of the Basic Law (BL48) include, inter alia, the power to appoint and remove judges of the courts at all levels. BL 88 further provides that the judges of the court of the HKSAR shall be appointed by CE on the recommendation of the Judicial Officers Recommendation Commission. That function reflects the role of CE under the Basic Law as head of the Hong Kong Special Administrative Region. Our current proposal for CE to appoint a panel of judges for authorizing interception of communications and the more intrusive covert surveillance is in line with that role and more generally the principle of executive-led government. There are many other statutory offices to which judges may be appointed, and CE is almost invariably the appointing authority[1]. The fact that they are appointed by CE in no way affects their independence in carrying out their statutory functions.

16. Moreover, as clearly provided for in the Bill, CE will only appoint the panel judges on the recommendation of the Chief Justice (CJ). As previously pointed out, prior to making the appointments, CE would ask CJ for recommendations. In other words, CE would only appoint someone recommended by CJ. The term of appointment would be fixed at three years, and we propose that CE would only revoke an appointment on CJ's recommendation and for good cause. There is no question of CE interfering with the consideration of individual cases or indeed the assignment of judges from within the panel to consider individual cases.

17. As set out in our earlier response to the questions raised by Members at the Panel meeting on 7 February 2006 (discussed at the Panel meeting on 16 February 2006), the proposed appointment arrangement would be comparable with the arrangement elsewhere for the appointment to be made by a senior member of the government. For example, in Australia, a Minister nominates the members of the Administrative Appeals Tribunal to approve interception of communications. In the UK, the Prime Minister appoints the Surveillance Commissioner for approving intrusive surveillance

---

[1] Examples include the chairmanship of the following: the Securities and Futures Appeals Tribunal under Cap 571; the Long-term Prisoners Sentences Review Board under Cap 524; the Post Release Supervision Board under Cap 475; the Administrative Appeals Board under Cap 442; the Market Manipulation Tribunal under Cap 571; and a Commission of Inquiry under Cap 86.

operations after they have been authorized by the executive authorities.

Relevant extracts from the Information Paper titled "Panel of Judges" for the meeting of LegCo Panel on Security on 7 March 2006

15. The Bill provides for comprehensive safeguards to cater for the special nature of the applications. These include, for example, the establishment of an independent oversight authority and the protection of products obtained from interception and covert surveillance operations. As far the panel judges are concerned, their independence is safeguarded with the proviso that CE may appoint them on CJ's recommendation, and for a fixed term. Since CE may only revoke the appointment during the term on CJ's recommendation and for good cause, there should not be any question of interference with their independence. More importantly, the security of their tenure as judges is never in question.

* * * * * *

Annex A3

Interception of Communications and Covert Surveillance

Need for a Panel of Judges

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 2 March 2006

Item 4: To explain the consideration factors or criteria adopted for proposing the appointment of a panel of judges by the Chief Executive for authorizing interception of communications and the more intrusive covert surveillance operations, and the differences between the aforementioned proposed framework and the framework for authorizing the issuance of search warrants by judges in terms of the role of judges, the procedures involved and the appeal or judicial review of the decisions of judges.

Item 5 : To explain why the Administration considers it appropriate for the Chief Executive to appoint a panel of judges for authorizing interception of communications and the more intrusive covert surveillance, and to clarify the functions of the panel judges, whether the decisions of the panel judges are subject to judicial review and whether the panel judges are subject to any rules or procedures of the court.

18. As regards the framework of the new regime, the Bill provides that a panel judge when carrying out his functions will act judicially, but not as a court or as a member of a court and that he will have all the powers and immunities of a judge of the High Court[2]. Conceptually this is not an unusual arrangement. For example, a Commissioner appointed under the Commissions of Inquiry Ordinance (Cap 86) will similarly not act as a court, although for all intents and purposes he will act judicially in carrying out his functions. Since a panel judge will not be acting as a court, he may be liable to judicial review in respect of his decisions. The Bill seeks to establish a self-contained statutory regime. In this respect the proceedings will not be generally subject to rights of appeal or other provisions of the High Court Ordinance or High Court Rules. The similarity with the issue of a

---

[2] In the case of *Bruno Grollo v. Michael John Palmer, Commissioner of the Australian Federal Police and Others F.C.95/032*, the Australian Court was of the view that issuing an interception warrant was a non-judicial power and as such held that a non-judicial function could not be conferred on a Judge without his or her consent.

subpoena or search warrant is only limited, in that the importance of the issues to be dealt with and their sensitivity are considerably different, hence justifying the setting up of the self-contained statutory regime that we have proposed.

Relevant extracts of Information Paper titled "Panel of Judges" for the meeting of LegCo Panel on Security on 7 March 2006

Need for self-contained regime

4. The Bill sets out a self-contained regime for granting judicial authorizations to cater for the sensitive and covert nature of interception of communications and covert surveillance. The regime is described in the papers that the Administration has prepared for discussion by Members on 7 and 16 February and 2 March 2006. The relevant extracts are at the **Annex** for Members' ease of reference.

not attached

5. At the meeting of the Panel of Security on 2 March 2006, some Members drew a comparison between the consideration of applications for authorization for interception of communications and covert surveillance by the panel of judges on the one hand, with the consideration of claims for public interest immunity (PII) and applications under various ordinances on the other, and asked if the judges would be exposed to the same level of sensitive information in both. We consider that the two are quite different.

6. At the outset, PII is only claimed in very limited circumstances during the course of proceedings which are already before the court. The classes of document or information for which PII has been claimed has included, for example, the identity of undercover police officers or informers, details of how surveillance operations have been carried out in a particular case, other details of law enforcement investigations, memoranda or minutes of meetings of the Executive Council and confidential financial advice. Although the judge may examine the documents or information to determine their relevance to the case, the prosecution, in a criminal case, or the Government as a party to civil proceedings, has the option of dropping the case or making admissions of fact, if the disclosure of the information would be extremely damaging to public interest or place a person in grave personal danger. Since 1992, when records began, only 27 PII certificates have been issued by the Chief Secretary.

7. Applications under the Organized and Serious Crime Ordinance (OSCO) relate to the production of materials, confiscation of proceeds of crime and search and seizures connected with organized and serious crime. Those under the United Nations (Anti-Terrorism Measures) Ordinance (UN(ATM)O) relate to specification and forfeiture of terrorist property[1]. The applications relate to one-off events, such as requesting an otherwise willing third party (e.g., a bank) who might otherwise be prevented from confidentiality requirements from providing readily available information, in much less covert circumstances (please also see paragraph 12 below).

8. As regards Part XII of the Interpretation and General Clauses Ordinance (IGCO), it relates to the production and search and seizure of journalistic material. Since the enactment of Part XII of IGCO in 1995, only three ex parte applications for warrants have been made.

9. Given that interception of communications and covert surveillance are indispensable investigation tools, the number of cases is necessarily much larger than, say, PII claims. We envisage the number of applications requiring judicial authorizations for these covert operations to be in the hundreds per year. The frequency and level of exposure of the panel judges to sensitive materials would be considerably higher as a result.

10. Another difference is the **identities of the parties**. A PII claim is made in the context of proceedings which have already started. Thus the judge will know the identities of all the parties, and will have an opportunity to consider on a case by case basis if the circumstances of the case require that he recuse himself from the case. Under the Bill, on the other hand, a panel judge will have no prior warning of the subject matter of an application, and will only discover the identity of the target (if known) when the application is made, by which time the security of the operation and of the material produced in support of the application might have been compromised.

11. Similarly, in OSCO and other ex parte applications to the court, the identities of the target is necessarily known. This is not always the case with interception of communications and covert surveillance operations —

---

[1] The relevant sections have yet to come into effect.

the identities of the target may in fact not always be known from the outset. For example, in a drug trafficking case, the identities of some of those involved may not be known at the beginning of the operation. Thus in such cases it would be far less practicable to deal with the sensitivity aspects on a case by case basis. Rather, we should seek to ensure that the system is designed to minimize any confidentiality risks at the outset.

12. The key difference between interception of communications and covert surveillance and other cases is that the former operations will **remain covert** and unknown to the target, and in many cases have to be kept confidential for a long time and sometimes indefinitely to, among other things, protect the identity or safety of personnel involved or ensure continued cooperation with other law enforcement agencies. With PII and other applications, the reverse is true – the operations either have become overt already or will become so almost immediately afterwards. In the case of claiming PII, there is an on-going trial and the question only turns on whether some information should be made available to the defence and / or the public. With respect to the application for a production order for journalistic material under IGCO, the application is made inter partes. In other cases, the operation will turn overt when the authorization is executed. The confidentiality and sensitivity concerns are therefore considerably less. Also, a range of judicial remedies such as appeals to the court would then apply. Where such remedies may not be available because of the continued covert nature of the operations, a self-contained regime is required.

13. The similarity between authorization of interception of communications and covert surveillance and the issue of a subpoena or search warrant, as suggested by some Members in our previous discussions, is in the Administration's view only limited. The considerations applicable to PII and coercive orders under the ordinances mentioned above are also applicable. Furthermore, the information provided to the magistrate is likely to be extremely brief and usually the warrant will be executed shortly after issue.

14. Under the system proposed in the Bill, the panel judges will have to consider applications for interception of communications and the more intrusive covert surveillance against the tests set out in the Bill and on the basis of the information that the LEAs have to provide in accordance with the Bill. The standards will necessarily be judicial ones. However, the panel

judges will not be sitting as a court. This means that the normal rules attendant on court proceedings will not apply. These rules include those governing legal representation, disclosure and appeal. The sensitive and covert nature of the applications necessarily makes these rules inapplicable.

15. The Bill provides for comprehensive safeguards to cater for the special nature of the applications. These include, for example, the establishment of an independent oversight authority and the protection of products obtained from interception and covert surveillance operations. As far the panel judges are concerned, their independence is safeguarded with the proviso that CE may appoint them on CJ's recommendation, and for a fixed term. Since CE may only revoke the appointment during the term on CJ's recommendation and for good cause, there should not be any question of interference with their independence. More importantly, the security of their tenure as judges is never in question.

* * * * * *

Annex A4

Interception of Communications and Covert Surveillance

Two-tier Approach in Authorization and Threshold for Covert Surveillance

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 5 : To explain the circumstances under which covert surveillance will be carried out by law enforcement agencies.

Item 6 : To explain how to differentiate between "more intrusive" operations and "less intrusive" operations under the two-tier authorization system for covert surveillance.

Item 7 : To illustrate by way of examples how the two-tier authorization system for covert surveillance works.

11. A note setting out the circumstances under which judicial and executive authorizations would be required in the case of covert surveillance operations is at **Annex B**.

12. We consider that the present scheme would provide very clear tests as to the circumstances under which different authorizations are required. Where there has been a change of circumstances requiring a different level of authorization, the appropriate authorization would need to be sought before an intended operation may be carried out. If both "more intrusive" and "less intrusive" surveillance is involved in a single operation, then judicial authorization would be sought.

13. Both types of covert surveillance would come under the purview of the Commissioner and would be subject to the same safeguards in respect of protection of products, etc. Furthermore, there are internal review mechanisms to ensure compliance with the relevant requirements. There is therefore little room for abuse.

Item 11 : To provide a list of offences where authorization should be given for covert surveillance and interception of communications respectively.

Item 12 : To provide information on the interception of communications and covert surveillance conducted by law enforcement agencies in terms of categories of offences.

17. We propose to set the threshold of the seriousness of offences by reference to an objective test – the maximum penalty for the offence. This approach is similar to that adopted in the 1996 LRC report, the 1997 White Bill and the IOCO. For covert surveillance, the threshold is offences with a maximum imprisonment term of at least 3 years or with a maximum fine of at least $1 million, and for interception of communications, offences with a maximum imprisonment term of at least 7 years. For comparison, the following summarizes the thresholds in the UK, Australia, and the United States (US) –

(a) the UK : in respect of interception and intrusive surveillance, offences for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to three years of imprisonment or more, or crimes that involve the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose;

(b) Australia : in respect of telecommunications interception, offences punishable by imprisonment for at least 7 years; in respect of surveillance, "relevant offences" include those punishable by imprisonment of 3 years or more, a few other specific offences, and offences prescribed by the regulations; and

(c) the US : in respect of interception of telecommunications and use of electronic surveillance devices, the list of offences enumerated in the Federal Wiretap Act s. 2516, where some offences are punishable by imprisonment for more than one year; in respect of interception of postal articles, all criminal activities.

18. Interception is considered to be a highly intrusive investigative technique and therefore a higher threshold is necessary. On the other hand, there is a wide spectrum of covert surveillance operations with varying degrees of intrusiveness. Also, since surveillance operations in general can

be more specific in terms of location, timing and event, they are less intrusive. On this basis, it seems reasonable to impose a lower threshold on the crimes over which such investigative technique could be deployed.

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

20. It is very important to bear in mind that the threshold is but an initial screen. Whether interception or covert surveillance may be authorized in each case has to be assessed against the proportionality and necessity tests.

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 21 February 2006

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.

Annexes A & B not attached

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.

Relevant Extracts from the Information Paper for the meeting of LegCo Panel on Security on 2 March 2006

Item 6. To consider the suggestion that some highly intrusive covert surveillance activities, for example the use of bugging device to pick up communications, should require a higher threshold as in the case of interception of communications which requires offences to be punishable with a maximum imprisonment of not less than seven years.

19. As set out in our previous responses, interception is considered to

be a highly intrusive investigative technique and therefore a high threshold is necessary. On the other hand, there is a wide spectrum of covert surveillance operations with varying degree of intrusiveness. Since surveillance operations can be more specific in terms of location, timing and event, the intrusiveness in terms of collateral intrusion to innocent party could be much lower. It would therefore be reasonable to include a wider spectrum of crimes against which the investigative technique of covert surveillance may be used, **where justified**.

20. In this connection, we would emphasize again that the limitation on the penalties of crime stipulated is only the initial screen and is by no way the only determining factor. In all cases, authorization would only be given if the tests of proportionality and necessity are satisfied. The relevant factors in considering the balancing test, as detailed in the Bill, include the immediacy and gravity of the crime, and the intrusiveness of the operation. Highly intrusive surveillance activities could only be justified where the crime concerned is sufficiently serious and where such threat is immediate.

* * * * * *

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

Definition of covert surveillance

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).

[Re: Annex A4]
Annex C to Information paper
on 21 February 2006

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 A5

Interception of Communications and Covert Surveillance

Renewal of Authorization

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 4 : To advise whether the renewal of judicial authorization would be indefinite, and if so, the justifications for that.

Related comments from the Criminal Law & Procedure Committee of the Law Society : The Committee has reservations on the 3 months' duration of authorizations and considers this to be too long for the initial authorization.

6. The three-month period proposed is the maximum duration that may be granted. The actual duration of the renewal would depend on the circumstances of each case and would have to be determined by the approving authority. Like a first-time application, an application for renewal would have to meet all the requirements regarding purpose, proportionality and necessity. In addition, it has to set out the benefits so far accrued from the operation and why a renewal is required.

7. Moreover, as with first-time authorizations, we would provide that once the purpose of the interception of communications or covert surveillance has been achieved or the conditions for the continuance of the authorization no longer apply, the operation has to be discontinued even if the renewal has not expired. The renewal then has to be revoked.

8. The maximum duration of three months is the same as that recommended in the 1996 LRC report and under the IOCO, and is the same as or less than the maximum duration allowed in Australia and the United Kingdom (UK) (ranging from 90 days to six months, depending on the nature of the cases).

9. Imposing a limit on the number of renewals could unnecessarily restrict the ability of LEAs to combat such crime as syndicated crime that usually requires a longer period of monitoring.

10. Paragraphs 6.125 to 6.129 of the 1996 LRC report discuss the duration question. They are extracted at **Annex A** for Members' ease of reference.

* * * * * *

Relevant Extract from the 1996 LRC report on interception on communications

Duration and renewal of warrants

6.125 Having determined the matters that must be made out to justify the issue of a warrant, the question of the warrant's duration requires consideration. We recommended in the consultation paper that a warrant should be issued for an initial period of 60 days. The Bar Association agreed that the period should be no longer than that. The Hon James To proposed that the period should be not more than 30 days so as to reflect the principle that interception is a last resort and should not be used unless it is absolutely necessary. Two other respondents commented that 60 days is too short and would like to see the duration extended to six months. Their concern is that investigations are often protracted and applying to court for renewal every two months would create inconvenience to the law enforcement agencies.

6.126 We are conscious that any decision on the length of warrant must be arbitrary. But the length is less of an issue than the arguments put forward by the applicant. If the applicant has a strong case, he can always come back to the court and apply for renewal. Nonetheless, we are concerned that the court might be burdened with unnecessary applications for renewal if the duration is as short as, say, 30 days.

6.127 We conclude that 90 days should suffice for both crime and public security. A similar period should govern extensions. In coming to this conclusion, we have considered the experience overseas. The position in other jurisdictions is summarised as follows:

(a) *Australia*

- 90 days if a criminal offence is involved;[47]
- Six months if the activities concerned are prejudicial to security.[48]

(b) *Canada*

- 60 days under the Criminal Code;[49]

---

47 Telecommunications (Interception) Act 1979 (Australia), section 49(3).
48 Telecommunications (Interception) Act 1979 (Australia), section 9(5).
49 Section 186(4)(e).

- 60 days or 1 year under the Canadian Security Intelligence Service Act 1984.[50]

(c) *Germany*

- Three months.[51]

(d) *New Zealand*

- 30 days for investigation of organised crime.[52]

(e) *South Africa*

- 90 days.[53]

(f) *United Kingdom*

- 60 days under the Interception of Communications Act 1985;[54]
- Six months under the Security Service Act 1989[55] and the Intelligence Services Act 1994.[56]

(g) *United States*

- 30 days.[57]

6.128 We have considered adoption of an upper limit to the number of extensions given, but have rejected this because each extension would have to be justified on the prescribed criteria.

6.129 **We recommend that a warrant should be issued for an initial period not exceeding 90 days and that renewals may be granted for such further periods of the same duration where it is shown (according to the same criteria applied to the initial application) to continue to be necessary.**

* * * * * *

---

50 Section 21(5).

51 Act on Restriction of the Secrecy of Mail, Posts and Telecommunications 1968, section 5(3).

52 Crimes Act 1961, section 312D(3).

53 Interception and Monitoring Prohibition Act 1992, section 3(3).

54 Section 4. It provides that warrants shall be issued for an initial period of 2 months and thereafter require renewal, also for a period of 2 months (but with provision for 6 months). Renewal requires that the Minister considers that the warrant "continues to be necessary" for the relevant purpose under section 2.

55 Section 3(4).

56 Section 6(2).

57 Wiretap Act, section 2518(5).

Annex A6

Interception of Communications and Covert Surveillance

Oral and Emergency Authorizations

Relevant extracts from theInformation Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 17 : To explain, quoting examples, the circumstances under which oral and very urgent applications (referred to in paragraph 17 of the Administration's paper for the meeting on 7 February 2006) would be made.

32. Oral applications could apply to both judicial and executive authorizations. They may be made in circumstances where a written application is not feasible, e.g., where a panel judge may be contacted by telephone but a hearing involving the applicant may otherwise not be feasible. Emergency authorizations apply only to cases which would otherwise require judicial authorization. We propose that the application should be made to the respective head of department who will not grant the authorization or renewal sought unless he is satisfied that it is not reasonably practicable, having regard to the urgency of the particular case, for the application to be submitted to the judge in accordance with the normal procedure. However, within 48 hours the application for confirmation must be made to a judge, who may revoke the approval. And as an additional safeguard, each case where the judge refuses to confirm the authorization would have to be reported to the Commissioner

33. The circumstances under which emergency applications could be considered should include imminent risk of death or serious bodily harm, substantial damage to property, serious threat to public security and loss of vital evidence. It is important for such procedure to be provided for in law so that the LEAs could arrange for emergency operations in well justified cases. We envisage that in practice emergency authorizations would only be resorted to sparingly and we anticipate that the Commissioner would wish to review such cases to ensure that the emergency application procedure is not abused.

* * * * * *

Annex A7

Interception of Communications and Covert Surveillance

Complaints Mechanism and Notification of Targets

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 16 : To advise whether any person whose communication sent to or by him has been intercepted by the law enforcement agencies or he himself is the subject of any covert surveillance operation would be informed of such activities conducted, and if not, the justifications for that.

30. In the 1996 LRC report, the LRC explained why it concluded against notification of targets of interception of communications. In essence, the LRC recognized the conflict between notification and the purposes of interception, which is necessarily clandestine. Notification could affect the operational effectiveness of LEAs. The prolonged retention of intercepted material arising from a notification requirement would have its own privacy risks. In addition, if the notification requirement is to be applied meaningfully, it will require the relevant authority to make an informed decision as to whether notification should be effected and the extent of information to be given to the target on a case by case basis. The resource implications are obvious. Also, destruction of the intercepted material prior to notification would largely destroy the basis of the notification mechanism. In line with the LRC's recommendation that material obtained through an interception of telecommunications shall be inadmissible in evidence, if intercepted material were destroyed and inadmissible in court, the risk of dissemination, and hence the risk to privacy, could be reduced to the minimum. We agree with the LRC's analysis and recommendations.

31. We note that neither the UK nor Australia has a notification arrangement. Given our policy in respect of the handling of telecommunications intercepts (see paragraphs 35 to 36 below), there is all the more reason not to notify the target. In covert surveillance cases where the product of covert surveillance would be able to be introduced into court proceedings, the product could be introduced into evidence or be disclosed as unused material, and the aggrieved person would be able to challenge it in court.

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 21 February 2006

Item 6 : To provide full justifications for not informing a person whose communication sent to or by him has been intercepted by law enforcement agencies or he himself is the subject of covert surveillance operation after such activities have been completed, or otherwise how the person could lodge complaint when he has not been informed of such activities.

15. We have set out our rationale of not informing targets of covert operations of such activities in paragraphs 30 to 31 of the paper presented to the Panel on Security on 16 February 2005. This is in line with the analysis and recommendations of the 1996 LRC report on regulating interception of communications, as well as the practice in the UK and Australia. We attach the relevant extract of the 1996 LRC report at **Annex D** for Members' ease of reference.

16. The European Court of Human Rights has found that the absence of a mandatory notification requirement after a covert surveillance operation is not a violation of the right to privacy. The Court considered that the threat against which surveillance were directed might continue for a long time after the operations. Thus notification to the individuals affected after the operations could compromise the long-term purpose that originally necessitated the surveillance. Such notification might reveal the modus operandi and fields of operation of law enforcement agencies and their agents.

17. A Member asked whether the unavailability of a notification procedure might undermine the effectiveness of the complaints handling system. According to our current thinking, the complaints handling mechanism under the proposed legislation would not impose the onus on the complainant to furnish the Commissioner with "proof" or information to substantiate his claim. Of course, the Commissioner may ask the complainant for information and the complainant may provide the Commissioner whatever information he considers relevant. More important, however, we plan to empower the Commissioner to obtain relevant information from those who may be able to provide it (who could be any public officer or any other person). As such, the absence of a notification arrangement would not affect the effective operation of the complaints

handling system.

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 2 March 2006

Item 3 : To reconsider the suggestion of notifying the targets of interception of communications or covert surveillance operations after such activities have discontinued, and applying to the court for not notifying the targets.

9. As explained in our previous papers, our current proposal of not notifying the targets of operations is in line with the analysis and recommendations of the 1996 LRC report on regulating interception of communications, as well as the practice in the United Kingdom and Australia. This is because threats being targeted by interception of communications or covert surveillance might continue for a long time after the operations. Thus notification to the individuals affected after the operation has ceased could still compromise the long-term purpose that originally necessitated the surveillance. Such notification might reveal the modus operandi and fields of operation of LEAs and their agents. In many cases this may ruin years of hard work and even subject the safety of LEA officers as well as those of the victims or witnesses to unnecessary risks. This would benefit criminal syndicates which are becoming increasingly organized and sophisticated.

10. Even for less sophisticated criminals, convictions are not necessarily the outcome of every operation. A notification requirement could greatly reduce the chance of successfully conducting the same surveillance operation on the same criminal again.

11. From a privacy point of view, a notification requirement would logically require relevant materials to be kept for the purpose of notification and any subsequent complaints arising. This would result in the need for related materials to be kept, and is contrary to the principle of destruction of such materials as early as possible to protect privacy.

12. As explained in the paper for the Panel's discussion on 21 February 2006, the complaints handling mechanism would not impose the onus on the complainant to furnish the Commissioner with "proof" or information to substantiate his claim. The Commissioner would be empowered to obtain relevant information from those who may be able to provide it (who may be

any public officer or any other person). As such, the absence of a notification arrangement would not affect the effective operation of the complaints handling system.

13. It should be emphasized that notification is only one of the safeguards against abuse. With other safeguards in the Bill as explained in our papers for the Panel's discussion on 7, 16 and 21 February, we consider that the present package represents a balanced approach in protecting the privacy of the individuals as well as ensuring the effectiveness of LEAs in carrying out their duties to protect the public. The jurisprudence of the European Court of Human Rights also supports the view that the absence of a mandatory notification requirement after a covert surveillance operation is not necessarily a violation of the right to privacy, and that safeguards should be seen in their totality. We believe that, viewed as a whole, the various safeguards included in our proposals are adequate and compare favourably with that in many common law jurisdictions.

* * * * * *

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.

7.73 Secondly, the individual should be able to challenge the grounds on which the

---

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.

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.

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.

---

[21] E.g. the participation of a "friend of the court".

[22] *R v Preston* [1993] 4 All ER 638 at 648. It is a case on the interception of telephone communications.

(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 risk to 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.

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.

---

[23] We recognise that "destruction" is not an absolute concept in the digital age.

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.

* * * * * *

Annex A8

Interception of Communications and Covert Surveillance

The Commissioner

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 15 : To consider establishing a committee as an independent oversight authority to keep under review law enforcement agencies' compliance with the provisions of the legislation regulating interception of communication and covert surveillance and any code of practice made under the legislation.

28. Our recommendation is in line with the recommendation in the 1996 LRC report in this respect. The Commissioner would be responsible for both ensuring compliance and examining complaints. Given the nature of work involved and to underline the independence of the authority, we consider that a person with judicial experience at a senior level should be appointed. We therefore propose that the law stipulate that either serving or retired judges at or above the level of the Court of First Instance of the High Court may be appointed as the authority.

29. Appointing a single person as a statutory authority is a common practice either in Hong Kong or overseas. For example, in Hong Kong the Ombudsman and the Privacy Commissioner are statutory authorities. In the UK, the oversight authority is the Interception of Communications Commissioner. In Australia, the Ombudsman performs the oversight function. As with the Privacy Commissioner or the Ombudsman, our proposed Commissioner will be supported by sufficient staff for him to discharge his functions.

* * * * * *

Annex A9

Interception of Communications and Covert Surveillance

Sanctions and Code of Practice

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 8 : To advise on the consequences of illegal covert surveillance conducted by law enforcement agencies.

Item 9 : To consider adding penalty provisions for non-compliance with any code of practice made under the proposed legislation.

14. We have proposed that the current exercise be limited to Government entities. This means that non-Government parties would not be subject to the regulation proposed. It would create an anomaly if, for the same conduct, law enforcement officers but not others would be subject to a new criminal offence. We will consider the need for introducing new criminal offences at the next stage. Under our proposal, a breach under the proposed legislation would be subject to disciplinary action, and this would be stipulated in the code of practice. An officer who deliberately conducts operations without due authorization might also commit the common law offence of misconduct in public office. In addition, any non-compliance would be subject to the scrutiny of the Commissioner, who may report such cases of irregularity to the heads of department and to the Chief Executive (CE), and who would handle complaints. Statistics on such cases would also be provided to CE in the Commissioner's annual report, which would be tabled in LegCo. These are powerful measures to ensure that LEAs and their officers will comply with the law and the applicable procedures.

15. Separately, all public officers have to observe the full range of existing laws. For example, the Telecommunications Ordinance provides for various offences in relation to the wilful interception of messages (sections 24) and damaging telecommunications installations with intent (section 27). The Post Office Ordinance has provisions governing the unauthorized opening of postal packets (sections 27 and 29). Other laws such as the Personal Data (Privacy) Ordinance may also be relevant. For a fuller summary of existing laws that may be applicable, please see Chapter 2 of the 1996 LRC report.

Item 10 : To advise whether the code of practice made under the legislation is subsidiary legislation.

16. The basic principles of the regime would be set out in the law. Amendments to these would necessarily have to be passed by LegCo. We do not consider it advisable for the Code of Practice covering operational details, which may need to be changed from time to time, to be made statutory. Our proposed legislation would stipulate that the Commissioner may make recommendations to the Secretary for Security on the Code or propose amendments thereto, thereby providing a considerable degree of oversight in respect of the content of the Code. Furthermore, the Code would be published and hence subject to public scrutiny.

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security 21 February 2006

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.

* * * * * *

Annex A10

Interception of Communications and Covert Surveillance

Protection of Information Obtained

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 2 March 2006

Item 1 : To advise whether there will be any provisions prohibiting the use of information obtained by interception of communications or covert surveillance for other purposes and how compliance with such provisions will be monitored.

2. The Interception of Communications and Surveillance Bill (the Bill) sets out in detail the safeguards for the disclosure and retention of interception or covert surveillance products (protected products). Under the Bill, disclosure of protected products or their copies is required to be kept to the minimum that is necessary for the relevant purpose of the prescribed authorization. Something is necessary for the relevant purpose of the prescribed authorization only if it continues to be, or is likely to become, necessary for the purpose sought to be furthered by carrying out the operation concerned or (except in the case of telecommunications interception) if it is necessary for the purposes of any pending or anticipated civil or criminal proceedings.

3. Within each law enforcement agencies (LEAs), arrangements would be made to minimize the extent to which protected products are disclosed or copied, or are subject to unauthorized or accidental access, processing, erasure or other use, and to ensure their proper destruction for the protection of privacy. This would help avoid misuse of the products of the operations in question.

4. The proposed regime would have a stringent review system, by both the Commissioner on Interception of Communications and Surveillance (the Commissioner) as well as internally, to ensure compliance with the new legislation and any code of practice that may be made under the legislation. Externally, reviews would be conducted by the Commissioner, who would be a sitting or former judge at or above the level of the Court of First Instance. He would examine compliance and propriety in respect of the information supplied in an application for authorization, the execution of the

authorization and the implementation and observance of various safeguards to protect the operation and information gathered. The Commissioner would also be able to refer any irregularity to the respective head of department, the Chief Executive or the Secretary for Justice. Internally, the head of the LEAs concerned would be required to make arrangements to keep under regular review the compliance by officers of the department with the relevant requirements, including the provisions of the legislation, code of practice and the requirements under the authorizations given.

5. Moreover, as explained in our response to questions raised by Members at the Panel meeting on 16 February 2006, under our proposed regime, there will be powerful sanctions against non-compliance. An officer who breaches the proposed legislation would be subject to disciplinary proceedings. An officer who deliberately conducts operations without due authorization may also commit the common law offence of misconduct in public office.

6. In their totality, the measures set out above provide a strong system ensuring compliance of LEA officers with the strict requirements regarding the disclosure and retention of protected products from interception or covert surveillance.

* * * * * *

Annex A11

For information
7 March 2006

Legislative Council Panel on Security
Interception of Communications and Covert Surveillance
Pre-Appointment Checking

Introduction

At the meeting of the Panel on Security of the Legislative Council (LegCo) on 2 March 2006, Members requested the Administration to explain in greater detail the checking to be conducted on panel judges prior to their appointment under the Interception of Communications and Surveillance Bill (the Bill).

Standard Arrangements for Protecting Information

2. For the covert law enforcement operations under discussion, it is essential to have operational arrangements to protect the information about the operations and the materials collected from the operations, so as to minimise the risk of leakage of intelligence, operational details, personal information etc. Apart from measures to ensure the physical security of documents and products, we need to ensure that access to such information and materials is restricted to the minimum number of persons, and that there is as little risk as possible of any disclosure, from such persons, that is not in line with the purpose of the operation. To this end, it has been our operational practice to require all Government officers with access to protected information to go through checking.

3. This practice will continue for Government officers under our proposed regime for the covert operations in question. In line with this practice, and to ensure the continued integrity of the system, we intend to conduct similar checks on the panel judges, the oversight authority and their respective staff.

4. Checking is not a sign of distrust of the person. On the contrary, it is because a person is trusted that he or she is considered for appointment to the position of, say, a Principal Official, the Commissioner of Police, or a panel judge under our proposal. The purpose of the checking is to confirm that trust, and minimize any risks for the system, the information under protection, and the persons themselves.

5. The operational need for checking prospective appointees to the proposed panel (and the oversight authority and their staff) before their appointment, is separate from the questions of whether there should be a panel of judges or who should appoint them. For the above operational reasons, whoever appoints the judges to our proposed panel, we would need the judges to be checked to minimize the risk of disclosure of information and materials, on par with the LEA officers involved, the oversight authority and his staff. (Our separate paper "Interception of Communications and Covert Surveillance – Panel of Judges" reiterates our thinking behind the arrangements for the Chief Executive (CE) to appoint a panel of judges.)

6. The following provides background information on the practice of checking.

Background

7. It is a long-standing and standard arrangement for checks to be conducted to ascertain the risks, if any, that might be involved in the appointment of an individual to a certain position. It is a routine procedure for various Government appointments, including appointments to civil service posts and to certain advisory and statutory bodies. The need for and types of checking required will depend on the particular circumstances of each individual case and take into account, among other things, the level and type of information to which the prospective appointee may have access and other relevant factors such as the frequency with which he may have access to such information, and the degree of control he may have over such information. Given its nature, the checking is normally done at the end of the appointment process when the candidate is considered suitable in all other respects.

8. As pointed out at the Security Panel meeting on 2 March 2006, the subject of "Integrity Checking for Disciplined Forces" has been the subject of discussion of the Panel on Security. Copies of the relevant papers submitted by the Administration for the May 2004 Panel meeting on the subject are at **Annex A**. In response to the concerns of Members regarding the related issue of checking of persons to be appointed to advisory and statutory bodies, to be Justices of the Peace and Principal Officials, upon the request of Members, supplementary information was subsequently provided to Members (a copy of the subsequent information paper is at **Annex B**).

not attached

not attached

9. As can be seen from the Annexes, broadly speaking there are three levels of checking : appointment checking, normal checking and extended checking, with the last one being the most extensive. Extended checking

is applicable to all people to be appointed to the most senior positions in the Government, e.g., Principal Officials and senior civil servants. It is also applicable to those who have access to very sensitive information. This is the checking that we have been doing for law enforcement officers with wide access to the more sensitive information arising from covert operations and will do for panel judges, the oversight authority, and their staff.

10. In extended checking, the prospective appointee will be requested to provide information on his personal particulars, educational background, social activities, employment history and family members. He will also be asked to nominate two referees. The checking will comprise interviews with the prospective appointee, his referees and supervisors as well as record checks. The checking is therefore much more thorough in order to help the appointment authority assess if there is any possible risk in appointing a candidate to a position involving much sensitive information. It **does not involve** any form of political vetting, and no investigation will be conducted on the political beliefs or affiliations of a prospective appointee.

11. Extended checking does not focus only on the "integrity" per se of the prospective appointee. There may well be factors unrelated to a person's personal "integrity" and beyond their control (for example, association of family members), that may expose them to a greater risk of, say, possible conflict of interests, than would otherwise be the case. In the case of the panel judges under discussion, there should not be doubts about their "integrity", but it is not inconceivable that a person is suitable to be a judge but circumstances are such that, without any reflection on his "integrity", it would not be appropriate for him to sit or continue to sit on the panel. Partly for this reason, and as mentioned in our previous papers, the Bill provides for CE to revoke the appointment of a panel judge on the Chief Justice's recommendation and for good cause.

12. We understand that at present, all Court of First Instance judges have been subject to criminal record checks and ICAC record checks prior to their appointment.

Position of the Judiciary

13. The Judiciary has stated its position on the subject as follows –

> "The Judiciary's position is that under the proposed legislation, the Chief Justice's recommendation of panel judges to the Chief Executive would only be based on professional criteria. The Administration's proposal is that before the appointment by the Chief Executive, the panel judges would undergo integrity

checking.

The Judiciary understands that any person with access to such highly sensitive materials has to undergo integrity checking and that there is no question that political vetting is involved. And the Judiciary has indicated to the Administration that it has no objection to its proposal."

Security Bureau
March 2006

Annex A12

Interception of Communications and Covert Surveillance

Evidential Use

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

Item 18 : To provide a written response to the issues raised in the letter dated 7 February 2006 from The Law Society of Hong Kong.

34. The response of the Administration set out above should address all issues covered in the Law Society's letter save for the issue on evidential use of telecommunication intercepts. ***The Society has indicated that its Criminal Law & Procedure Committee has reservations on the proposed destruction of material. They are of the view that the normal rule of disclosure should apply and the defence should have a right of disclosure to any unused material.***

35. The LRC has set out its analysis on the evidential use and admissibility of telecommunications intercepts in the 1996 LRC report. The relevant extract is at **Annex C**. We agree with the LRC's analysis and recommendations.

36. Since neither the prosecution nor the defence may adduce any evidence from telecommunications intercepts, there is equality between the two sides in this respect. In a recent ruling of a case (in the case of Mo Yuk-ping on 23 August 2005), the court was satisfied that the policy adopted by the Government of allowing telecommunications intercepts for intelligence gathering only and thereafter requiring the destruction of the product to be rational, striking an acceptable balance between various competing interests. *[re: para. 83 and 88 of Judge Wright's ruling]* Having said that, to cater for any exceptional cases, we would also provide in the legislation that disclosure should be made to the judge where the fairness of the trial so requires.

37. Safeguards are provided at different stages of the process to ensure fairness. All authorizations for interception operations would be given by members of a panel of judges. There are also a number of safeguards in our

proposals regarding, for example, the need to protect the confidentiality of intercepts products, limiting access to these materials, etc. The execution of the authorization, including the compliance with safeguards, would also be subject to review by the Commissioner.

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 21 February 2006

Item 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.

* * * * * *

Relevant Extracts from the 1996 LRC report on interception on communications : Evidential Use and Admissibility

Admissibility of material obtained through interception of communications carried out pursuant to a warrant

7.23 The adoption of section 6 of the 1985 Act will have the result that evidence of the fruits of *authorised* interception of telecommunications can never be produced in court. The intercepted material and the copies thereof must be destroyed once its purpose (e.g. the prevention or detection of crime) has been served. However, a party might be in breach of the requirement to destroy the material and seek to adduce it in evidence. Further, the statutory requirements for destruction would not apply to material obtained by an authorised interception of communications other than telecommunications, or an interception which was not authorised by the court.

7.24 Under general common law principles, the admissibility of evidence is solely determined by the relevance of the evidence. The court has no power to exclude evidence merely because the judge disapproves of the way in which it was obtained, as, for example, where evidence was obtained unfairly or by trickery.[6] There is, however, a judicial discretion to exclude evidence if its prejudicial effect exceeds its probative value. The court also has inherent jurisdiction to make orders which are necessary to ensure a fair trial.

7.25 In determining whether to admit intercepted material in evidence, we need to take into account the probative value of the material and the privacy risk involved. High quality evidence collected by means which pose a low privacy risk should be admissible but low quality evidence collected by means which pose a high privacy risk should be inadmissible. Other factors include the purpose of the interception, the duration of the warrant, and the amount of relevant and irrelevant information obtained from the interception.

7.26 The sub-committee initially considered that intercepted material pertaining to the period preceding the laying of the charge should be admissible in the subsequent prosecution. Restricting the admissibility of evidence obtained as a result of an interception would have far-reaching results. It would mean that even if an interception reveals the sole evidence of a serious offence, that evidence may not be adduced.

---

6 *R v Cheung Ka-fai* [1995] HKLR 184 at 195. The test of admissibility of evidence in Hong Kong is governed by the common law as expressed in *R v Sang* [1980] AC 402 at 432-3.

Similarly, evidence which assists an accused, such as an attempt to fabricate evidence against him, may not be adduced if it was obtained by interception, even though the interception was authorised by the court.

Material obtained through interception of telecommunications

7.27 While evidence arising from interception of telecommunications is not usually admitted in Hong Kong, in a recent major drug case it was.[7] We note that the laws of the United States,[8] Canada,[9] and Australia[10] regulating the interception of telecommunications all countenance the admission of lawfully intercepted material as evidence in prosecutions.

7.28 We recommended at the beginning of this chapter that material obtained by an interception of telecommunications should be destroyed as soon as its prescribed purpose has been fulfilled. Admitting in evidence material obtained through an interception of telecommunications would require its retention for this purpose. This would run counter to our recommendation on destruction of intercepted material. It also gives rise to the problem of disclosure of unused material to the defence. Generally, only a small part of the intercepted material would be used by the prosecution as evidence. But since the prosecution is under a duty to disclose all material information, all unused material would probably have to be made available to the defence.[11]

7.29 It is true that the court may impose appropriate conditions. For example, defence counsel may have to undertake not to divulge the contents of tapes played to them. But use of intercepted material as evidence will necessarily compound the invasion of privacy entailed in the original intrusion. There is always a risk of *public* dissemination of personal information contained in the intercepted communications. Furthermore, the present legal status of unused material is vexed and is subject to a number of appeals.

7.30 A further complication which is avoided by prohibiting the use of intercepted material as evidence arises from the application of public interest immunity.

7.31 In view of the risk of public dissemination of intercepted information and the difficulties with disclosure of unused material, the sub-committee recommended in the consultation paper that material obtained through an interception of communications should be inadmissible as evidence, regardless of its relevance.

---

7 *R v Cheung Ka-fai* [1995] HKLR 184. The calls in that case were intercepted by the Royal Canadian Mounted Police.

8 Wiretap Act, sections 2515 and 2518(9) & (10)(a).

9 Criminal Code, section 189(5). Notice of intention to introduce evidence of lawfully intercepted communications must be given to the accused.

10 Telecommunications (Interception) Act 1979, section 74.

11 *R v Preston* [1993] 4 All ER 638 at 664. The test for whether unused material should be disclosed by the prosecution to the defence is materiality, not admissibility.

7.32 Implementing the recommendation in the consultation paper necessitates the adoption of a provision similar to section 9 of the United Kingdom Interception of Communications Act 1985. This section prohibits any reference to authorised or unauthorised interception of telecommunications and mail. Subsections (1) and (2) state:

> *"(1) In any proceedings before any court or tribunal no evidence shall be adduced and no question in cross-examination shall be asked which (in either case) tends to suggest -*
>
> *(a) that an offence under section 1 above has been or is to be committed by any of the persons mentioned in subsection (2) below; or*
>
> *(b) that a warrant has been or is to be issued to any of those persons.*
>
> *(2) The persons referred to in subsection (1) above are -*
>
> *(a) any person holding office under the Crown;*
>
> *(b) the Post Office and any person engaged in the business of the Post Office; and*
>
> *(c) any public telecommunications operator and any person engaged in the running of a public telecommunication system."*

7.33 It appears that section 9(1) would not prevent the admission of evidence and cross-examination in the exceptional cases where there can be an interception without an offence being committed (e.g. because of consent) where no warrant is in existence.

7.34 The United Kingdom Government hoped that by making intercepted material generally inadmissible in legal proceedings, it would ensure that interception could be used only as an aspect of investigation, not of prosecution.[12] However, the Court of Appeal in *Effik* held that section 9 does not provide that evidence obtained as a result of an interception would be inadmissible:

> *"The forbidden territory is drawn in a much narrower fashion. And there is a logical reason for the narrow exclusionary provision. That is the reflection that it cannot be in the public interest to allow those involved in espionage or serious crime to discover at a public trial the basis on*

---

[12] *Interception of Communications in the United Kingdom* (Cmnd 9438, 1985), clause 12(f).

> *which their activities had come to the notice of the Police, the Customs and Excise or the Security Services, such as, for example, by questions designed to find out who provided the information which led to the issue of the warrant. So interpreted section 9(1) makes sense. And it would make no sense to stretch that language to become a comprehensive exclusion of all evidence obtained as a result of any interception."*[13]

7.35 The Court of Appeal in *Preston* agreed that section 9 does not operate to render inadmissible in evidence the contents of the intercepts. However, the effect of a literal application of the language of section 9(1) would, other than possibly in the most exceptional case, be to prevent any material derived from an interception being adduced in evidence. The court explained:

> *"In order to lay the groundwork for material to be admissible in evidence the manner in which the material has been obtained will normally have to be given in evidence in court and this will in turn tend to suggest either an offence under section 1 has been committed or a warrant has been issued which therefore contravenes section 9. It is this evidence of how the material was obtained which is the 'forbidden territory' and the fact that it should not be adduced in evidence will also usually prevent the material which was obtained as a result of the interception being given in evidence."*[14]

7.36 The result is that it is normally not possible to adduce any evidence obtained as a result of an interception to which the 1985 Act applies. Such a prohibition would cover not only the fruits of interception but also the manner in which the interception was carried out. But if the parties were by agreement or admission to put the material before the court, it appears that there is nothing in section 9 to prevent this.[15]

7.37 In Hong Kong there is no bar to the defence raising the issue of interception, provided it is relevant to the case. In practice, it is extremely rare for material obtained through interception of telecommunications to be used as evidence in court. A provision in similar terms to section 9 would render any reference to interception activities

---

13 *R v Effik* (1992) 95 Cr App R 427 at 432.

14 *R v Preston* (1992) 95 Cr App R 355 at 365.

15 The House of Lords explained that this point is of little or no importance in practice because if the regulatory system is working properly the material will have been destroyed long before the trial, and if it is favourable to the accused the prosecution will not have been pursued: *R v Preston* [1993]4 All ER 638 at 672. As section 6 of the 1985 Act requires the destruction of intercepted material once a charge is laid against the accused, the purpose of section 9 can be seen as the protection, not of the fruits of the interception, but of the information as to the manner in which they were authorised and carried out: *op cit,* at 667.

inadmissible, whether or not it was authorised. As far as interception of telecommunications is concerned, this would mean that no evidence could be adduced and no question could be asked in cross-examination, which tended to suggest that an offence in relation to the interception of telecommunications had been committed or that a warrant authorising an interception of telecommunications had been issued.

7.38 One respondent to the consultation paper was concerned that the proposal on inadmissibility would preclude the suspect from confronting the basis of an investigation. The suspect might have contended that the intercepted communication had been misinterpreted by the law enforcement agency and, as a result of that mistake, the agency had triggered an elaborate investigation leading to his prosecution. We reiterate that the intercepted material would be used only for intelligence and not as a basis for the decision whether or not to prosecute. Although the suspect would not have an opportunity to correct any mistake made by the agency in compiling the analyses, he would still be able to confront in court the admissible evidence collected on the basis of the intercepted material should a prosecution ensue.

7.39 The Bar Association found it unsatisfactory that lawfully obtained material which may be the only evidence of a crime cannot be used at trial, but instead has to be destroyed. They preferred a regime which would allow the prosecution to decide whether, and to what extent, material obtained pursuant to a warrant is retained and used.

7.40 Other respondents also had reservations on our proposals. The Hong Kong Alliance of Chinese and Expatriates held the view that judges should see as much evidence as was available, particularly when it would be the court which would authorise any intrusion. The Alliance wanted to see a regime in which the prosecution must reveal that intrusive measures had been applied. The Liberal Democratic Federation of Hong Kong was concerned that the work of the law enforcement agencies would be hindered and the deterrent effect weakened if material obtained by interception was inadmissible. They therefore proposed to give the court a discretion to admit such material as evidence depending on its usefulness.

7.41 There were, however, others who agreed with the proposal that intercepted material should be inadmissible. One respondent commented that the legislation should expressly provide that intercepted material should be exempted from pre-trial disclosure to the defence. We agree with this comment in principle. We understand that the law enforcement agencies are satisfied that the adoption of the proposal regarding inadmissibility of intercepted material would not undermine their efforts in fighting crime. Indeed, making intercepted material inadmissible would protect the safety of those who are engaged in covert activities because details of the conduct of an interception would not be made public.

7.42 Material gleaned from an interception is often not specific. Since interception of telecommunications normally lasts for weeks or even months, it is highly likely that personal information which is not relevant to the investigation would be acquired. Much of the information obtained by investigators would probably relate to "innocent" parties who have had contacts with those targeted for interception. If the intercepted material were admissible, this would inevitably result in an invasion of the privacy both of innocent parties and of the target himself. From a privacy point of view, the person whose privacy has been affected by an interception ought to be notified that his right to privacy has been infringed. Problems relating to notification then arise. Who should be notified of an interception? Of what should he be notified? Under what circumstances should he be notified? And when should he be notified? All these problems could be avoided if the privacy of the person affected by an interception could be safeguarded by the destruction of the intercepted material and the rendering of that material inadmissible in court.

7.43 The preceding discussion explains that the principal purpose of interception of telecommunications is the *gathering of intelligence*, and not the collection of evidence for use in prosecutions. It will be recalled that one of the grounds for the issue of warrants is the "prevention or detection" of serious crime, not the "prosecution" of serious crime. As interception of telecommunications (including telephone tapping) poses a high privacy risk but normally generates material of low probative value, we maintain that material obtained through an interception of telecommunications should be inadmissible in evidence.

7.44 **We recommend that material obtained through an interception of telecommunications carried out pursuant to a warrant shall be inadmissible as evidence regardless of its relevance. For the purposes of this recommendation, "telecommunications" means communications by electromagnetic means. This prohibition should cover not only the fruits of interception but also the manner in which the interception was made.**

7.45 **We recommend that no evidence shall be adduced and no question shall be asked in cross-examination which tends to suggest that an offence in relation to an interception of telecommunications has been committed or that a warrant authorising an interception of telecommunications has been issued.**

* * * * * *

Annex A13

Interception of Communications and Covert Surveillance

Resources Implications of the Legislation Proposals

Relevant extracts from the Information Paper for the meeting of LegCo Panel on Security on 2 March 2006

Item 7. To advise on the resource implications on law enforcement agencies of the implementation of the proposed legislation.

21. The proposals to establish an authorization authority and an independent oversight authority together with a complaint mechanism involving the payment of compensation will have financial and staffing implications. The LEAs would also have to deploy resources to put in place the new system within their departments. We are still assessing the resource implications more fully, and will do so in parallel with the discussion of the Bill with LegCo. We will try to meet the additional requirements from existing resources if possible and will seek additional resources where necessary in line with established procedures.

* * * * * *

Annex A14

政 府 總 部
香 港 下 亞 厘 畢 道

GOVERNMENT SECRETARIAT
LOWER ALBERT ROAD
HONG KONG

本函檔號 OUR REF.: SBCR 3/2/3231/94
來函檔號 YOUR REF.: CB2/PL/SE

Tel: 2810 2474
Fax: 2523 1685

Urgent By Fax: 2509 0775

25 February 2006

Mrs Sharon Tong
Clerk to LegCo Panel on Security
Legislative Council
3/F Citibank Tower
3 Garden Road
Central

Dear Mrs Tong,

Interception of Communications and Covert Surveillance

Number of Cases

I refer to paragraph 3 of the Administration's paper that the Panel discussed on 21 February 2006. The law enforcement agencies have in the past few days undertaken a quick review of the cases of interception of communications and covert surveillance in the last three months of 2005. The number of cases is as follows –

- Interception of communications : 178
- Covert surveillance : 170

We have previously explained that the current regulatory regime for interception of communications and covert surveillance is different from our proposed regime in various ways. For example, the thresholds for the definition of crime warranting the use of covert surveillance is any crime at present but would be serious crime[1] for the proposed regime. Applying

[1] offences punishable by a maximum of 3 years' imprisonment or above or a fine of $1 million or above

the criteria of the proposed new legislative regime to these cases, the number of cases of interception of communications that would require judicial authorization would be 178. As regards covert surveillance, 28 cases would require judicial authorization and 114 cases executive authorization. The remainder (28 cases) are accounted for by the differences between the two regimes.

I should be grateful if you would bring this to Members' attention.

Yours sincerely,

(Miss Cheung Siu Hing)
for Secretary for Security