For information
16 February 2006

Legislative Council Panel on Security

Interception of Communications and Covert Surveillance

Response to issues raised by Members at the meeting of 7 February 2006

Introduction

This paper sets out the Administration's response to issues raised by Members at the meeting of the Panel on Security of the Legislative Council (LegCo) on 7 February 2006. The numbering of items follows that set out in the revised list of issues attached to the letter of 9 February 2006 from the Clerk to Panel.

Responses to issues raised

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

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

3. We have referred to "public security" in our proposals as it is the term used in Article 30 of the Basic Law. As can be seen from the 1996 Law Reform Commission (LRC) Report on interception of communications (the 1996 LRC report), the 1997 White Bill on Interception of Communications and the 1997 Interception of Communications Ordinance (IOCO), the approach generally is to leave

the term "public security" undefined so that security cases are considered and justified on their own individual circumstances. All applications must satisfy the tests set out in the law. All interceptions and more intrusive covert surveillance operations would have to be approved by a member of the panel of judges. In addition, all such operations would be subject to oversight by the proposed Commissioner on Interception of Communications and Surveillance (the Commissioner).

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

4. During this first stage of the exercise, we seek to authorize and regulate the conduct of our law enforcement agencies (LEAs) and we would in fact be specifying those departments under the law. Non-government entities would not be dealt with at this stage under our current proposals. For similar activities of parties other than those of the Hong Kong Special Administrative Region Government, they are subject to current laws (statutes and common law) that apply to all persons in Hong Kong (please see paragraph 15 below). They will also be subject to any future laws that may be made in this and other related areas. In this connection, the following studies the LRC has done or is doing may be relevant –

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

These issues may be dealt with separately.

Item 3 : To consider providing in the legislation that reasons for interception of communications or covert surveillance should be included in the application for judicial authorization, and such application should be made by way of an affidavit.

5. We agree that all applications for authorization should be supported by sufficient reasons, and propose to list the information required in the legislation. As regards the form, our current thinking is that an affidavit would be required for judicial authorizations and a declaration would be required for executive authorizations.

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

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

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

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

8. The maximum duration of three months is the same as that

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

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

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

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

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

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

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

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

13. Both types of covert surveillance would come under the

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

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

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

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

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

applicable, please see Chapter 2 of the 1996 LRC report.

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

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

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

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

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

(a) the UK : in respect of interception and intrusive surveillance, offences for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be

sentenced to three years of imprisonment or more, or crimes that involve the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose;

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

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

18. Interception is considered to be a highly intrusive investigative technique and therefore a higher threshold is necessary. On the other hand, there is a wide spectrum of covert surveillance operations with varying degrees of intrusiveness. Also, since surveillance operations in general can be more specific in terms of location, timing and event, they are less intrusive. On this basis, it seems reasonable to impose a lower threshold on the crimes over which such investigative technique could be deployed.

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

necessity are met, covert surveillance could be used to prevent and detect such offences.

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

Item 13 : To provide statistics on the "more intrusive" and "less intrusive" covert surveillance operations carried out by law enforcement agencies.

21. We have tried to see if it is possible to compile the relevant figures, but have found it very difficult to do so. The existing system is very different from the proposed one. Previously there have been no uniform reporting requirements across the LEAs for publication, and no classification as presently proposed. As a result, we have not adopted a uniform system of keeping past statistics, and it would be impracticable to work out the figures post-hoc. With interception of communications, in line with long-standing policy, the records are destroyed within a fairly short time to protect privacy and are no longer available. For covert surveillance, even if the records are still available, a mammoth effort would be required to go over the records for a number of years to prepare the figures for them to be meaningful.

22. Looking ahead and for the purpose of consideration of our proposed regime, it is relevant that :

(a) there would be uniform classification of operations, which would enable the preparation of uniform statistics; and

(b) the proposed legislation would specify information that has to be included in the proposed Commissioner's report to CE, which would be tabled in LegCo. Such information would include the number of authorizations and renewals issued, the number of applications that have been refused and a summary

of reviews conducted by the Commissioner, etc.

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

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

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

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

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

25. Judges appointed to the panel will receive no advantages from that appointment. They will continue to be judges and whatever they do while on the panel will in no way affect their continued eligibility as judges. That they are appointed by CE to the panel therefore would give no positive or negative incentives that might affect their independence when carrying out their duties as judges on the panel.

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

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

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

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

29. Appointing a single person as a statutory authority is a common practice either in Hong Kong or overseas. For example, in Hong Kong

the Ombudsman and the Privacy Commissioner are statutory authorities. In the UK, the oversight authority is the Interception of Communications Commissioner. In Australia, the Ombudsman performs the oversight function. As with the Privacy Commissioner or the Ombudsman, our proposed Commissioner will be supported by sufficient staff for him to discharge his functions.

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

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

31. We note that neither the UK nor Australia has a notification arrangement. Given our policy in respect of the handling of telecommunications intercepts (see paragraphs 35 to 36 below), there is all the more reason not to notify the target. In covert surveillance cases where the product of covert surveillance would be able to be introduced

into court proceedings, the product could be introduced into evidence or be disclosed as unused material, and the aggrieved person would be able to challenge it in court.

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

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

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

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

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

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

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

37. Safeguards are provided at different stages of the process to ensure fairness. All authorizations for interception operations would be given by members of a panel of judges. There are also a number of safeguards in our proposals regarding, for example, the need to protect the confidentiality of intercepts products, limiting access to these materials, etc. The execution of the authorization, including the compliance with safeguards, would also be subject to review by the Commissioner.

Security Bureau
February 2006

Annex A

Relevant Extract from the 1996 LRC report on interception on communications

Duration and renewal of warrants

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

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

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

(a) *Australia*

- 90 days if a criminal offence is involved;[1]
- Six months if the activities concerned are prejudicial to security.[2]

---

1 Telecommunications (Interception) Act 1979 (Australia), section 49(3).
2 Telecommunications (Interception) Act 1979 (Australia), section 9(5).

(b) *Canada*

- 60 days under the Criminal Code;[3]
- 60 days or 1 year under the Canadian Security Intelligence Service Act 1984.[4]

(c) *Germany*

- Three months.[5]

(d) *New Zealand*

- 30 days for investigation of organised crime.[6]

(e) *South Africa*

- 90 days.[7]

(f) *United Kingdom*

- 60 days under the Interception of Communications Act 1985;[8]
- Six months under the Security Service Act 1989[9] and the Intelligence Services Act 1994.[10]

(g) *United States*

- 30 days.[11]

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

---

3 Section 186(4)(e).
4 Section 21(5).
5 Act on Restriction of the Secrecy of Mail, Posts and Telecommunications 1968, section 5(3).
6 Crimes Act 1961, section 312D(3).
7 Interception and Monitoring Prohibition Act 1992, section 3(3).
8 Section 4. It provides that warrants shall be issued for an initial period of 2 months and thereafter require renewal, also for a period of 2 months (but with provision for 6 months). Renewal requires that the Minister considers that the warrant "continues to be necessary" for the relevant purpose under section 2.
9 Section 3(4).
10 Section 6(2).
11 Wiretap Act, section 2518(5).

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

* * * * * *

Annex B

Types of Covert Surveillance

Options for regulatory framework

In formulating our proposal for covert surveillance we have taken into account the discussion and recommendations in the 1996 consultation paper "Privacy : Regulating Surveillance and the Interception of Communications" of the Privacy Sub-Committee of the Law Reform Commission (LRC) (the 1996 LRC paper). In addition, we have taken reference from the regulatory regimes of comparable common law jurisdictions, in particular, that of Australia.

2. The **1996 LRC paper** recommends a regulatory framework comprising **three criminal offences** along these lines –

(a) entering private premises as a trespasser with intent to observe, overhear or obtain personal information therein;

(b) placing, using or servicing in, or removing from, private premises a sense-enhancing, transmitting or recording device without the consent of the lawful occupier; and

(c) placing or using a sense-enhancing, transmitting or recording device outside private premises with the intention of monitoring without the consent of the lawful occupier either the activities of the occupant or data held on the premises relating directly or indirectly to the occupant.

The 1996 LRC paper further recommends that **warrants be required to authorise** all surveillance within the scope of the proposed criminal offences.

3. On paragraph 2 (a), currently law enforcement agencies (LEAs) are already liable for trespass and any unlawful act that they may do on

the premises that they have trespassed. In practice, therefore, such operations are unlawful unless authorized under the law, e.g., by way of a search warrant. Our proposed legislation corresponds to the other two proposed criminal offences in paragraph 2 above, and other situations not discussed in detail in the 1996 LRC paper.

4. The regulatory regimes of **comparable common law jurisdictions** vary considerably. The United States (US) statutory regimes cover only the use of devices to monitor and record communications. The UK's statutory regime is more up to date and comprehensive, covering intrusive surveillance (where private premises are involved) and directed surveillance (covert surveillance other than intrusive surveillance). The UK regime provides for executive authorization of directed surveillance operations and approval of executive authorizations by a Surveillance Commissioner, who must be a sitting or former judge, of intrusive surveillance operations. We have taken greater reference from the legislation Australia enacted in 2004, which is the latest model among the jurisdictions that we have studied. Previously Australia's Commonwealth legislation covered only the use of listening devices. The 2004 legislation covers listening, data surveillance, optical surveillance, and tracking devices.

Our proposed regime

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).

Annex C

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

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

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

7.24 Under general common law principles, the admissibility of evidence is solely determined by the relevance of the evidence. The court has no power to exclude evidence merely because the judge disapproves of the way in which it was obtained, as, for example, where evidence was obtained unfairly or by trickery.[12] There is, however, a judicial discretion to exclude evidence if its prejudicial effect exceeds its probative value. The court also has inherent jurisdiction to make orders which are necessary to ensure a fair trial.

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

---

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

7.26 The sub-committee initially considered that intercepted material pertaining to the period preceding the laying of the charge should be admissible in the subsequent prosecution. Restricting the admissibility of evidence obtained as a result of an interception would have far-reaching results. It would mean that even if an interception reveals the sole evidence of a serious offence, that evidence may not be adduced. Similarly, evidence which assists an accused, such as an attempt to fabricate evidence against him, may not be adduced if it was obtained by interception, even though the interception was authorised by the court.

Material obtained through interception of telecommunications

7.27 While evidence arising from interception of telecommunications is not usually admitted in Hong Kong, in a recent major drug case it was.[13] We note that the laws of the United States,[14] Canada,[15] and Australia[16] regulating the interception of telecommunications all countenance the admission of lawfully intercepted material as evidence in prosecutions**.**

7.28 We recommended at the beginning of this chapter that material obtained by an interception of telecommunications should be destroyed as soon as its prescribed purpose has been fulfilled. Admitting in evidence material obtained through an interception of telecommunications would require its retention for this purpose. This would run counter to our recommendation on destruction of intercepted material. It also gives rise to the problem of disclosure of unused material to the defence. Generally, only a small part of the intercepted material would be used by the prosecution as evidence. But since the prosecution is under a duty to disclose all material information, all unused material would probably have to be made available to the defence.[17]

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

---

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

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

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

16 Telecommunications (Interception) Act 1979, section 74.

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

Furthermore, the present legal status of unused material is vexed and is subject to a number of appeals.

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

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

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

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

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

7.34 The United Kingdom Government hoped that by making intercepted material generally inadmissible in legal proceedings, it would ensure that interception could be used only as an aspect of investigation, not of prosecution.[18] However, the Court of Appeal in *Effik* held that section 9 does not provide that evidence obtained as a result of an interception would be inadmissible:

> *"The forbidden territory is drawn in a much narrower fashion. And there is a logical reason for the narrow exclusionary provision. That is the reflection that it cannot be in the public interest to allow those involved in espionage or serious crime to discover at a public trial the basis on which their activities had come to the notice of the Police, the Customs and Excise or the Security Services, such as, for example, by questions designed to find out who provided the information which led to the issue of the warrant. So interpreted section 9(1) makes sense. And it would make no sense to stretch that language to become a comprehensive exclusion of all evidence obtained as a result of any interception."*[19]

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

> *"In order to lay the groundwork for material to be admissible in evidence the manner in which the material has been obtained will normally have to be given in evidence in court and this will in turn tend to suggest either an offence under section 1 has been committed or a warrant has been issued which therefore contravenes section 9. It is this evidence of how the material was obtained which is the 'forbidden territory' and the fact that it should not be adduced in evidence will also usually prevent the material which was obtained as a result of the interception being given in evidence."*[20]

---

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

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

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

7.36 The result is that it is normally not possible to adduce any evidence obtained as a result of an interception to which the 1985 Act applies. Such a prohibition would cover not only the fruits of interception but also the manner in which the interception was carried out. But if the parties were by agreement or admission to put the material before the court, it appears that there is nothing in section 9 to prevent this.[21]

7.37 In Hong Kong there is no bar to the defence raising the issue of interception, provided it is relevant to the case. In practice, it is extremely rare for material obtained through interception of telecommunications to be used as evidence in court. A provision in similar terms to section 9 would render any reference to interception activities inadmissible, whether or not it was authorised. As far as interception of telecommunications is concerned, this would mean that no evidence could be adduced and no question could be asked in cross-examination, which tended to suggest that an offence in relation to the interception of telecommunications had been committed or that a warrant authorising an interception of telecommunications had been issued.

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

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

---

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

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

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

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

7.43 The preceding discussion explains that the principal purpose of interception of telecommunications is the *gathering of intelligence*, and not the collection of evidence for use in prosecutions. It will be recalled that one of the grounds for the

issue of warrants is the "prevention or detection" of serious crime, not the "prosecution" of serious crime. As interception of telecommunications (including telephone tapping) poses a high privacy risk but normally generates material of low probative value, we maintain that material obtained through an interception of telecommunications should be inadmissible in evidence.

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

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

* * * * * *