For information
2 March 2006

Legislative Council Panel on Security
Interception of Communications and Covert Surveillance

Response to issues raised by Members at the meeting of 21 February 2006

Introduction

This paper sets out the Administration's response to issues raised by Members at the meeting of the Panel on Security of the Legislative Council (LegCo) on 21 February 2006. The numbering of items follows that set out in the list of issues attached to the letter of the 24 February 2006 from the Clerk to Panel.

Responses to issues raised

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

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

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

4. The proposed regime would have a stringent review system, by both the Commissioner on Interception of Communications and Surveillance (the Commissioner) as well as internally, to ensure compliance with the new legislation and any code of practice that may be made under the legislation. Externally, reviews would be conducted by the Commissioner, who would be a sitting or former judge at or above the level of the Court of First Instance. He would examine compliance and propriety in respect of the information supplied in an application for authorization, the execution of the authorization and the implementation and observance of various safeguards to protect the operation and information gathered. The Commissioner would also be able to refer any irregularity to the respective head of department, the Chief Executive or the Secretary for Justice. Internally, the head of the LEAs concerned would be required to make arrangements to keep under regular review the compliance by officers of the department with the relevant requirements, including the provisions of the legislation, code of practice and the requirements under the authorizations given.

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

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

Item 2 : To advise whether there are any guidelines prohibiting suspects or witnesses from recording conversations with law enforcement officers, without the knowledge of the latter, during the taking of statements.

7. The Bill only regulates the conduct of public officers and people acting on their behalf in carrying out interception and covert surveillance. It would not affect the conduct of other individuals nor create any liability for them in this regard.

8. The Rules and Directions for the Questioning of Suspects and

the Taking of Statements (Rules and Directions), issued by the Secretary for Security, contain guidelines for LEA officers in the taking of statements from suspects in order to protect these suspects' rights. The suspects have the right to request a record of the interview. There is no specific provision in the Rules and Directions prohibiting the use of recording equipment by the suspects, nor are there any other law or guidelines against such acts. However, if the statement taking process occurs whilst a suspect is in custody, the question of recording should not arise because the suspect would not have access to his own recording device. In any case, suspects will be given a copy of all statements taken from them.

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

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

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

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

12. As explained in the paper for the Panel's discussion on 21 February 2006, the complaints handling mechanism would not impose the onus on the complainant to furnish the Commissioner with "proof" or information to substantiate his claim. The Commissioner would be empowered to obtain relevant information from those who may be able to provide it (who may be any public officer or any other person). As such, the absence of a notification arrangement would not affect the effective operation of the complaints handling system.

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

14. We attach at **Annex** the relevant extracts of our previous responses on the subject for Members' ease of reference.

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

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

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

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

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

18. As regards the framework of the new regime, the Bill provides that a panel judge when carrying out his functions will act judicially, but

---

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

not as a court or as a member of a court and that he will have all the powers and immunities of a judge of the High Court[2]. Conceptually this is not an unusual arrangement. For example, a Commissioner appointed under the Commissions of Inquiry Ordinance (Cap 86) will similarly not act as a court, although for all intents and purposes he will act judicially in carrying out his functions. Since a panel judge will not be acting as a court, he may be liable to judicial review in respect of his decisions. The Bill seeks to establish a self-contained statutory regime. In this respect the proceedings will not be generally subject to rights of appeal or other provisions of the High Court Ordinance or High Court Rules. The similarity with the issue of a subpoena or search warrant is only limited, in that the importance of the issues to be dealt with and their sensitivity are considerably different, hence justifying the setting up of the self-contained statutory regime that we have proposed.

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

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

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

---

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

activities could only be justified where the crime concerned is sufficiently serious and where such threat is immediate.

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

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

Security Bureau
March 2006

Annex

Interception of Communications and Covert Surveillance
Response to the Issue of Notification of Targets by the Administration

Extract of Information Paper for the meeting of LegCo Panel on Security on 16 February 2006

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

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

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

Extract of Information Paper for the meeting of LegCo Panel on Security on 21 February 2006

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

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

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

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

Annex D to Information Paper
on 21 February 2006

Relevant Extracts from the 1996 LRC report on interception on communications : Notification

Notification following termination of interception

The notification requirement

7.70 A requirement that the object of interception be notified of the fact that he had been subject to interception once it is terminated is a feature of some but not all laws. In the United States, the Wiretap Act requires that "the persons named in the order or application, and such other parties to intercepted communications as the judge may determine" be notified of the period of interception and such portions of the intercepted communications as the judge may determine.[18] The Canadian Criminal Code also provides that the person who was the object of an authorised interception be notified of that fact. The notice, however, need not include the contents or details of the authorisation.[19] In Germany, "[m]easures of restriction shall be notified to the person concerned after they are discontinued".[20]

7.71 Merely to inform an individual of the fact that he has been the object of interception would serve little purpose. More helpful and informative would be to notify the former target of the sorts of matters covered by the United States provision, including, where appropriate, providing portions of the intercepted communications themselves. We understand that under current Hong Kong practice often only key points from the intercepted communications will be abstracted and retained.

The basis of notification requirement

7.72 The basis of a notification requirement is two-fold. First, it marks the seriousness of the earlier intrusion into privacy. The requirement would introduce an important element of accountability and should deter the authorities from intercepting unnecessarily.

---

18 Section 2518(8)(d).

19 Section 196.

20 German Act on Restriction of Privacy of Mail, Posts and Telecommunications 1989, section 5(5). Indeed one aspect of the German law which was challenged in *Klass* is that there was no requirement that the object of interception be *invariably* notified upon its cessation. The European Court held that this was not inherently incompatible with the privacy provision of the European Convention, provided that the person affected be informed as soon as this could be done without jeopardising the purposes of the interception.

7.73 Secondly, the individual should be able to challenge the grounds on which the intrusion was allowed. Denying the target information that he has been the object of interception will limit the efficacy of the mechanisms enhancing accountability, such as review procedures and the provision of compensation awarded for wrongdoing. We note that the United Kingdom Act lacks a notification requirement and, although compensation is provided for, no claim to date has been successful.

7.74 We think that the public has a right to be told the extent to which intrusions are occurring, although this would partly be addressed by the public reporting requirements to be recommended by us in the next chapter. The adoption of a notification requirement would diminish the need for mechanisms at the stage when the warrant is approved, such as the participation of a third party in the *ex parte* proceedings to represent the interests of the target.[21] There are, however, practical problems in implementing this requirement.

Practical problems of notification

(a) The conflict between notification and the purposes of interception

7.75 A notification requirement would have to be made subject to a proviso ensuring that the operational effectiveness of law enforcement agencies would not be diminished. The requirement would have to be couched in terms that, following the termination of interception, the targets and, perhaps, those innocent parties affected by the interception, should be notified unless this would "prejudice" the purposes of the original intrusion. There would also need to be provision for postponement of the notification on the same grounds.

7.76 "Prejudice", in relation to the target, could be defined to cover the situation where the target is likely to be the object of surveillance or interception in the future and notification is likely to make such surveillance or interception more difficult. This approach would preclude notification of recidivist offenders, or those where there is a reasonable prospect that the investigation may be reopened in the future.

7.77 In the case of notification of "innocent" persons, the most obvious ground on which notification would be denied is if they could be expected to alert the target. Another possibility is that the authorities may wish to tap the innocent person in order to further tap the target again and alerting the innocent person may make this more difficult.

---

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

7.78 The United Kingdom approach is that interception is necessarily clandestine and merely divulging that it has occurred would diminish the value of interception.[22] This obviously runs counter to any requirement of notification.

(b) Prolonged retention of intercepted material

7.79 If part of a notification requirement is to be that details of the fruits of an interception are to be disclosed following the termination of the interception, this necessarily implies that those materials must be retained. This has its own privacy risks.

(c) Resource implications

7.80 If the notification requirement is to be applied meaningfully, it will require the relevant authority to make an informed decision as to whether notification should be effected, applying criteria along the lines described above. Consideration would need to be given to the extent of information to be given to the target under a notification requirement. This raises potentially complex issues and would require the relevant authority to be well briefed on a case by case basis, applying the prejudice test outlined above. The resource implications are obvious. We recommend below that decisions impinging on interceptions should be capable of review. If decisions regarding notification are similarly to be reviewed, the resource implications will be even greater.

The need for notification

7.81 We have recommended that material obtained through interception of telecommunications shall be destroyed immediately after the interceptions have fulfilled the purpose. Destruction of the intercepted material prior to notification would largely destroy the basis of the notification mechanism.[23]

7.82 We have also recommended that material obtained through an interception of telecommunications shall be inadmissible in evidence. If intercepted material were destroyed and inadmissible in court, the risk of dissemination, and hence the riskto privacy, could be reduced to the minimum. There is therefore less need for a notification requirement in Hong Kong than in other jurisdictions where intercepted material may be produced at the trial.

---

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

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

7.83 We note that the practice in the United States and Canada is only to notify the public of the fact of interception. It is presumably due to this that those jurisdictions do not appear to have encountered the difficulties we envisage may result from a more extensive notification requirement. We think that a restricted notification requirement along the lines of that in the United States and Canada is of little benefit. Finally, we believe that the accountability aspect is more directly addressed by the warrant system and the public reporting requirement. We have therefore concluded that a person whose telecommunications have been intercepted need not be notified of the interception.

7.84 As regards material obtained by an interception of communications transmitted other than by telecommunication (for example, letters and facsimile copies), although they will not be subject to a destruction requirement and will continue to be admissible in court, we do not think that any privacy problems arise. If the material was adduced in evidence, the suspect would have a right to challenge it in court; and if the material was not required or no longer required for any criminal proceedings, it should have been returned to the addressee or the sender, as the case may be, unless this would prejudice current or future investigation. Further, where one of the parties to the communication is aggrieved by the interception, he may ask for a review under the procedures recommended in Chapter 8 below. It is therefore not necessary for the persons communicating other than by telecommunication to be notified of the fact that his communications had been intercepted or interfered with.

7.85 In conclusion, it is not necessary to provide for a requirement that the object of an interception of communications be notified of the fact that he had been subject to interception. In coming to this conclusion, our main concerns are that such a scheme would have considerable resource and privacy implications, without a clear concomitant benefit. The only exception to this conclusion is where a warrant has been set aside by a judge or the supervisory authority concludes that a warrant had been improperly issued or complied with. We shall explain this in detail in Chapter 8 below.

* * * * * *