For information
7 March 2006

Legislative Council Panel on Security

Interception of Communications and Covert Surveillance
Panel of Judges

Introduction

This note sets out issues relating to the panel of judges for authorizing interception of communications and more intrusive (i.e. Type 1) surveillance operations under the new regime proposed in the Interception of Communications and Surveillance Bill (the Bill).

The current regime

2. The responsibility for investigating crime and protecting the public from security threats falls primarily on the executive. Interception of communications and covert surveillance have been indispensable investigatory tools to ensure that the law enforcement agencies (LEAs) may carry out their duties in protecting the public effectively. Hitherto authorizations for these operations have been given by the executive.

Introducing judicial authorization

3. In line with increased public expectation for enhanced transparency, accountability, and checks and balances in the operation of the Government, and developments in international jurisprudence in human rights, we accept that enhanced safeguards for the more intrusive operations would be necessary. One way of achieving this would be by vesting the power of authorization to a body independent of the executive. After detailed consideration, we have come to the view that this should be achieved by entrusting this function to senior members of the Judiciary.

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.

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 — 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

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

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.

Conclusion

16. In conclusion, the Administration is of the view that as far as the regime for the authorization of interception of communications and covert surveillance operations is concerned, it is important that there is a self-contained system to uphold confidentiality. At the same time, there should be sufficient safeguards to protect the privacy of individuals. By providing for a self-contained system with a panel of experienced judges to consider applications for interception of communications and the more intrusive covert surveillance, plus the built-in safeguards regarding the tests to be applied and an independent oversight authority, the Bill seeks to achieve a proper balance in this regard.

Security Bureau
March 2006

Annex

Extracts from Information Papers provided to the Panel on Security on the Need for Self-contained Regime

Extract of the paper for the meeting of Panel on Security on 7 February 2006

21. The authority for authorizing all interception of communications and the more intrusive covert surveillance operations would be vested in one of a panel of judges. Members of the panel would be appointed by the Chief Executive (CE) based on the recommendations of the Chief Justice (CJ). The panel would consist of three to six judges at the level of the Court of First Instance of the High Court. To ensure consistency and to facilitate the building up of expertise, panel members would have a tenure of three years and could be reappointed.

Extract of the paper for the meeting of 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.

Extract of the paper for the meeting of 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[2]. 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

---

[2] 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.

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 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[3]. 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.

---

[3] 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.