立法會
Legislative Council

LC Paper No. CB(2)2245/10-11(02)

Ref : CB2/PL/SE

Panel on Security

Background brief prepared by the Legislative Council Secretariat for the meeting on 5 July 2011

Review of the Interception of Communications and Surveillance Ordinance and intelligence management

Purpose

This paper gives background information and summarizes relevant discussions of the Panel on Security ("the Panel") on the review of the Interception of Communications and Surveillance Ordinance (Cap. 589) ("ICSO") and intelligence management.

Background

Interception of Communications and Surveillance Ordinance

2. According to Article 30 of the Basic Law, the needs of public security and the investigation of criminal offences are the only two grounds on which relevant authorities may inspect communications in accordance with legal procedures. ICSO, which came into force on 9 August 2006, provides for a stringent regulatory regime for the interception of communications and specified kinds of covert surveillance operations by public officers, to ensure that the law enforcement agencies ("LEAs") pay attention to and observe the privacy and other rights of the public while they combat crimes and protect public security.

3. Safeguards for privacy are provided under ICSO at various stages of operations conducted by LEAs, from the initial application, execution of the authorization, to the subsequent oversight. The salient features of the regulatory and monitoring mechanism established under ICSO are outlined in the following paragraphs.

Authorization

4. Before LEAs carry out any interception operations, they must first obtain an authorization from an authorizing authority which is either a panel judge appointed in accordance with ICSO or a designated senior LEA officer. While a judge's authorization is required for "more intrusive" covert surveillance operations, the authorizing authority for "less intrusive" covert surveillance operations is a senior officer of the LEA concerned.

Conditions for authorization

5. The conditions for authorization are strictly defined under section 3 of ICSO. The purpose of the operation must be confined to the prevention or detection of serious crimes or the protection of public security. Where serious crime is concerned, ICSO sets different thresholds for interception of communications and covert surveillance. Since the degree of intrusiveness of interception of communications is generally higher, only offences for which the maximum penalty is imprisonment of not less than seven years count as serious crime. As for covert surveillance, offences that count as serious crime is imprisonment of not less than three years or a fine of not less than one million dollars. In addition, the tests of proportionality and necessity must be met, including the requirement that the purpose of the operation cannot reasonably be fulfilled by other less intrusive means.

Execution

6. During the execution of an authorization, LEAs must ensure that the conditions for the continuance of a prescribed authorization are complied with. ICSO also requires LEAs to continuously review the situation.

Products of operation

7. The materials obtained by interception of communications and covert operations may contain sensitive private information about the targets and other innocent persons. Improper use or disclosure of such materials would result in a serious infringement of their privacy. ICSO therefore strictly regulates the handling of such materials by LEAs. ICSO expressly requires heads of LEAs to make arrangements to ensure that the extent to which such materials are disclosed, the extent to which they are copied and the number of such copies made should be limited to the minimum that is necessary; that all practicable steps are taken to ensure that such materials are protected against unauthorized or accidental access, processing or erasure; and that such materials are destroyed as soon as their retention is not necessary for the relevant purpose of

the authorization.

Oversight mechanism

8. In addition to the various safeguards mentioned above, throughout the entire process (whether before, during or after the operation), the compliance of LEAs with the relevant requirements is subject to independent oversight as well as LEAs' regular internal reviews. ICSO especially provides for a Commissioner on Interception of Communications and Surveillance ("the Commissioner"), who is a serving or former judge of the Court of First Instance or Court of Appeal, or a former permanent judge of the Court of Final Appeal.

9. The Commissioner has the power to review all relevant records of LEAs, to require any public officer or other person to answer any question and provide information, and to require any officer to prepare a report on any case. The Commissioner may make recommendations to the heads of LEAs, and to the Secretary for Security on what should be included in the Code of Practice issued by the Security Bureau ("SB") under section 63 of ICSO for the purpose of providing practical guidance to law enforcement officers in respect of matters specified under ICSO. If deemed necessary, the Commissioner may report to the Chief Executive ("CE"), the Secretary for Justice, or one of the panel judges appointed under ICSO. LEAs are under a statutory obligation to report to the Commissioner any irregularities under ICSO.

10. The Commissioner also acts on complaints to determine whether any interception or covert surveillance has been carried out without proper authority. He may notify the applicant if he has found in the applicant's favour and order the Government to pay compensation. Furthermore, he may give notice and award compensation to the subject of an operation which has been carried out without proper authority even where the subject has not made any complaint. This serves as another powerful incentive for LEAs to comply with the relevant requirements.

11. ICSO provides that the Commissioner must submit an annual report to CE, who will cause it to be tabled before the Legislative Council ("LegCo"). The report will cover such matters as the various aggregate statistics and the compliance of LEAs with the relevant requirements of ICSO.

Deliberations of the Panel

12. Since the commencement of ICSO on 9 August 2006, the Commissioner has submitted four annual reports to CE, the Panel had discussed the results of

the Administration's study of matters raised in the annual reports at six meetings and the Administration's review of ICSO at its meeting on 6 July 2010. The major views and concerns raised by members are summarized below.

Appointment of senior judges as panel judges

13. Some members strongly opposed the present arrangements of appointing senior judges as panel judges for the purpose of considering applications for prescribed authorizations to conduct interception and covert surveillance operations. Expressing concern about the implications of the appointment arrangements, including the role and independence of the panel judges, they urged the Administration to address the issue in the comprehensive review of ICSO.

14. According to the Administration, checks and balances were built into the ICSO regime to ensure that a balance was maintained between protecting the privacy of individuals and allowing LEAs to conduct interception and covert surveillance operations for the purpose of prevention and detection of serious crimes and protection of public security in warranted circumstances. Whenever an application was made to the relevant authority (panel judge or authorizing officer) for a prescribed authorization, the relevant authority would assess whether the conditions for the issuance of the prescribed authorization as set out in ICSO were met.

Protection of information subject to legal professional privilege and proactive monitoring of interception products and related records

15. Members were concerned whether the Administration would, in considering the Commissioner's recommendations to amend ICSO, solicit views from LEAs and the Department of Justice. They noted that the Administration had formed an interdepartmental working group ("the Working Group") to conduct a comprehensive review of ICSO. In undertaking the review, the Administration would take into account the recommendations of the Commissioner, the views of panel judges and the operational experience of LEAs.

16. Members considered it necessary to strike a balance between protecting privacy and legal professional privilege ("LPP"), while allowing LEAs to carry out interception of communications and covert surveillance operations for the prevention or detection of serious crimes and the protection of public security.

17. According to the Administration, it recognized the need to strike a balance between combating serious crimes and protecting the privacy of individuals. Stringent safeguards were provided under ICSO at all stages of the covert operations, from the initial application to the execution of the authorization, and throughout the entire oversight process. Regarding the review of ICSO, as a number of the issues involved the panel judges, the Working Group would consult the panel judges. In conducting the review, the Administration would strive to improve the operation of the ICSO regime without compromising the privacy of individuals and the effectiveness of LEAs in combating serious crimes. The Working Group would take into account the comments of members, panel judges and the Commissioner in formulating the recommendations.

18. There was a view that during the process of reviewing and considering legislative amendments to ICSO, the Administration should consult the public widely on the proposed amendments. The Administration advised that it was still in the process of reviewing the entire ICSO. In considering whether legislative amendments to ICSO were required, it would take into account the views of relevant parties, including the Commissioner, the panel judges, members and LEAs, as well as the views of the two legal professional bodies where appropriate.

19. There was a call for the expansion of the content of the Commissioner's annual report to include the numbers of applications received from and authorizations issued or renewed for respective LEAs, as well as more detailed information on renewal cases.

20. According to the Administration, it was concerned that the provision of too much information in the Commissioner's annual report might reveal the investigation capability of LEAs, and would be prejudicial to the prevention and detection of crime and the protection of public security. Notwithstanding, the Administration would refer members' request to the Commissioner for consideration.

Review of panel judge's determination

21. Noting the Administration's proposal to establish a mechanism for the review of a panel judge's determination of an application for the issue of a judge's authorization, members sought information on the rationale and the implementation details for the proposal. According to the Administration, ICSO did not provide for any mechanism for an LEA to apply to a panel judge for a review of the latter's determination. In 2008, the numbers of interception authorizations issued and applications for the issue of interception

authorizations refused were 801 and 13 respectively. The Administration planned to explore the option of establishing a statutory review mechanism under which a panel judge might, upon application by an LEA, review his own determination. It considered that this arrangement would enable LEAs to have an opportunity to explain to the panel judges their grounds for making the applications in person and to provide further information about their applications where necessary.

Commissioner's power and authority to listen to interception product and the need for legislative amendments

22. Some members were concerned whether the Administration would amend ICSO to enable panel judges and the Commissioner to access interception products. Some other members were however concerned that allowing the Commissioner or his designated officers to check interception products might increase the risk of disclosure or leakage of confidential information.

23. According to the Administration, there was an absence of express and unambiguous provisions in ICSO empowering the Commissioner to listen to interception products. It was also doubtful whether section 53(1)(a) regarding the power of the Commissioner to require any person to provide information for the purpose of performing his functions under ICSO could be construed as having the effect of empowering the Commissioner to listen to interception products. With the existence of legal uncertainty, the Commissioner considered that the safest way was to amend ICSO to allow the Commissioner and the staff designated by him to conduct the checking. The Administration would carefully consider the recommendations raised in the Commissioner's annual reports, including the one in connection with the Commissioner's authority to listen to interception products which required legislative amendments for implementation, during the comprehensive review of ICSO.

24. The Administration further advised that it fully respected the need to facilitate the performance of the panel judges' and the Commissioner's functions under ICSO. However, the public must be assured that the proposed arrangements would not add intrusion into their privacy, infringe their right to confidential legal advice or increase the risk of unauthorized disclosure or unintended leakage. It would consult panel judges and the Commissioner on the detailed proposals.

Differences in the interpretation of provisions in the legislation

25. Members were concerned that LEAs and panel judges held different interpretations on a number of provisions in ICSO, such as the power of panel

judge to revoke an authorization that had been granted, to impose additional conditions when confirming an emergency authorization and to revoke a device retrieval warrant. Some members were concerned whether LEAs were challenging the rule of law, the power of panel judges and the views of the Commissioner. They took the view that if LEAs questioned the power of the panel judge to revoke the prescribed authorization, LEAs should seek remedy from the court, such as to quash the panel judge's decision of revocation or his refusal to allow the continuance of the prescribed authorization or to seek for a declaration of a proper interpretation of the statutory provision.

26. The Administration responded that although the annual reports revealed occasional disagreement between LEAs and the Commissioner on the interpretation of certain provisions of ICSO, there was no question of LEAs being disrespectful to panel judges or the Commissioner. LEAs had adopted pragmatic measures to address the Commissioner's concerns and resolve the differences in views between them regarding the power of panel judge to revoke an authorization. SB had also amended the Code of Practice where appropriate to address the issues identified in the annual reports. As some of the Commissioner's recommendations arose from different interpretations of certain provisions in ICSO, the Administration would consider those recommendations in detail when it conducted the comprehensive review of ICSO. The review would provide an opportunity for the Administration to identify further legislative improvements to ICSO.

Possibility of expanding the scope of the review on ICSO

27. Some members were concerned about the reasons for not legislating against interception of communications and covert surveillance activities carried out by organizations such as the agencies of the Central People's Government in the Hong Kong Special Administrative Region, and not providing express provisions in ICSO to guard against public officers' non-compliance.

28. According to the Administration, existing legislation afforded some protection from interference with private communications by non-public officers. For example, section 24 of the Telecommunications Ordinance (Cap. 106) provided that it was an offence for any person who had official duties in connection with a telecommunications service to willfully destroy, alter, intercept or detain any message intended for delivery, or to disclose any message to any person other than the person to whom the message was addressed; and section 27 stipulated that a person who damaged, removed or interfered with any telecommunications installation with intent to intercept or discover the contents of a message was guilty of an offence. Under both sections, a person convicted of the relevant offence was liable on summary

conviction to a fine of $20,000 and to imprisonment for two years. Furthermore, there were provisions in the Post Office Ordinance (Cap. 98) and the Personal Data (Privacy) Ordinance safeguarding the privacy of individuals in relation to postal packets and personal data.

29. Members also sought information on whether the Administration would expand the scope of its review on ICSO to cover the following issues -

(a) to consider expanding the definition of intercepting act and covert surveillance, with a view to enhancing the protection for Hong Kong residents' right to freedom and privacy of communications;

(b) to re-examine the appropriateness of setting up a panel judges system and conferring non-judicial powers on panel judges to issue or grant prescribed authorizations for interception or covert surveillance;

(c) to consider involving other relevant parties, such as the Privacy Commissioner for Personal Data, in the process of granting authorization since views from third parties, particularly from human rights and privacy perspectives, would be relevant to the panel judge's determination of the authorization;

(d) to consider introducing penalty provisions to guard against law enforcement officers' non-compliance with ICSO or CoP, and to consider making the use of privileged information obtained through interception of telecommunications for any purposes a criminal offence;

(e) to consider instituting a mechanism whereby LEAs, panel judges and the Commissioner could seek declarations from the court if they held different interpretations on any provisions in ICSO; and

(f) to consider establishing a mechanism for the keeping and destruction of intelligence derived from interception of communications and covert surveillance activities.

30. According to the Administration, -

(a) ICSO was enacted after thorough deliberations in the Legislative Council. During the Committee stage of the Interception of Communications and Surveillance Bill, it had provided detailed explanation regarding the definitions of intercepting act and covert

surveillance, as well as the need to appoint panel judges to consider applications for authorizations;

(b) ICSO was intended to provide for a stringent regulatory regime for the interception of communications and the use of surveillance devices by public officers, in particular to ensure that LEAs respected the privacy and other rights of the public while combating crimes and protecting public security;

(c) the report on "Privacy: Regulating the Interception of Communications" released by the Law Reform Commission ("LRC") in 1996 recommended that it should be an offence for a person to intentionally intercept or interfere with communications in the course of their transmission, other than where authorized by a warrant. Separately, in its report on "Privacy: The Regulation of Covert Surveillance" released in 2006, LRC recommended the creation of two new criminal offences to prohibit the obtaining of personal information through trespass on private premises or by means of a surveillance device. While the conduct of interception of communications and the use of surveillance devices by public officers was regulated by ICSO, the Administration was of the view that it should not draw any conclusion lightly that the conduct of non-public officers in this respect should be regulated. As a matter of fact, the two LRC reports were highly controversial. When they were published, the Hong Kong media sector and journalists expressed worry that the recommendations might compromise press freedom. In view of the wide public concern over the issue, the Administration would not accept the recommendations lightly. In determining the way forward, the Administration would consider carefully how press freedom and privacy could be maintained at the same time. At the present stage, the Administration did not have any plan to introduce legislation to implement the LRC recommendations;

(d) any public officer who had committed an act in contravention of the provisions in ICSO or CoP would be subject to disciplinary action under the disciplinary mechanism of the department concerned. Any public officer who had intentionally conducted interception of communications or covert surveillance without lawful authority was liable to be prosecuted for the common law offence of misconduct in public office;

(e) during the monitoring process, the Commissioner and LEAs had identified a few cases of non-compliance with the relevant requirements of ICSO. Some of them involved technical errors and some were due to individual officers' failure to thoroughly understand or be familiar with the requirements. The Commissioner had indicated in his annual reports to CE that he was satisfied with the overall performance of LEAs and their officers in their compliance with the requirements of ICSO, and that he had not found any wilful or deliberate flouting of such requirements;

(f) the Commissioner had also pointed out in his Annual Report 2008 that the panel judges were vigilant and strict in their consideration of applications by LEAs for interception and surveillance, and he had not found a single case in 2008 in which he entertained any doubt as to the propriety of their determination, be it a grant of a prescribed authorization or a refusal; and

(g) as regards the controls over intelligence obtained through interception or covert surveillance, LEAs would take into account various factors, including the need for continued retention and information accuracy, in determining whether certain information captured by their intelligence systems should continue to be kept. Intelligence generated from such information would be destroyed when their retention was no longer required.

Review of the intelligence management system of LEAs

31. The Panel noted that in examining the Interception of Communications and Surveillance Bill, members of the Bills Committee had expressed concern over LEAs' intelligence management system and there was a suggestion that sufficient safeguards should be put in place to prevent possible abuse of retention and use of intelligence derived from interception of communications and covert surveillance activities. Some members called on the Administration to establish a mechanism for the keeping and destruction of intelligence derived from such activities, and to review the existing intelligence management system of LEAs.

32. The Administration advised that information obtained in the course of a duly authorized interception of communications or covert surveillance operation might be kept as intelligence if it was related to the prevention and detection of crime or the protection of public security, so as to assist LEAs in performing

their functions. All law enforcement officers must abide by the Hong Kong Bill of Rights Ordinance (Cap. 383), the Personal Data (Privacy) Ordinance (Cap. 486) and ICSO. In addition, all LEAs had put in place a stringent intelligence management system. With regard to the keeping of intelligence, LEAs would take into account factors such as the need for continued retention and information accuracy in determining whether certain information captured by their intelligence systems should continue to be kept. During the scrutiny of the Interception of Communications and Surveillance Bill, the Administration undertook to conduct a comprehensive review of the existing intelligence management system of LEAs in a separate exercise with a view to further strengthening the systems, particularly to enhance the transparency of the policy on the use of such information. The review of LEAs' intelligence management system had commenced and consultation with LEAs concerned was in progress. The Administration aimed to report to the Panel on the outcome of the review in around July 2011.

Relevant papers

33. A list of the relevant papers on the Legislative Council website is in the **Appendix**.

Council Business Division 2
Legislative Council Secretariat
30 June 2011

Appendix

Relevant papers on
Review of the Interception of Communications and Surveillance Ordinance and intelligence management

Committee	Date of meeting	Paper
Legislative Council	1.3.2006	Official Record of Proceedings (Question 4)
Panel on Security	6.11.2007 (Item V)	Agenda Minutes
Panel on Security	6.12.2007 (Item I)	Agenda Minutes
Panel on Security	16.2.2009 (Item I)	Agenda Minutes
Panel on Security	3.3.2009 (Item IV)	Agenda Minutes
Legislative Council	11.3.2009	Motion on "Reviewing the Interception of Communications and Surveillance Ordinance"
Panel on Security	7.12.2009 (Item I)	Agenda Minutes
Panel on Security	6.7.2010 (Item III)	Agenda Minutes
Panel on Security	29.11.2010 (Item I)	Agenda Minutes

Council Business Division 2
Legislative Council Secretariat
30 June 2011