立法會
Legislative Council

LC Paper No.CB(2)2431/04-05(01)

Ref : CB2/PL/SE

Panel on Security

Background brief prepared by the Legislative Council Secretariat for the special meeting on 15 August 2005

Regulation of surveillance and the interception of communications

Purpose

This paper summarises the discussions so far held by Members on the regulation of surveillance and interception of communications.

Background

Existing provisions regulating surveillance and interception of communications

2. Interception of communications is currently regulated under the Telecommunications Ordinance (Cap. 106) and Post Office Ordinance (Cap. 98). Under section 33 of the Telecommunications Ordinance, the Chief Executive (CE) may, if he considers that the public interest so requires, order that any message brought for transmission shall not be transmitted, or that any message brought for transmission, or transmitted, or received or being transmitted, shall be intercepted or disclosed to the Government. Under section 13 of the Post Office Ordinance, the Chief Secretary for Administration may grant a warrant authorising the Postmaster General or any officer of the Post Office to open and delay any postal packet.

The Law Reform Commission' report on regulating the interception of communications

3. In April 1996, the Law Reform Commission (LRC) published a consultation paper entitled "Privacy: Regulating Surveillance and the

Interception of Communications" for public consultation for two months. In December 1996, LRC published a report entitled "Privacy: Regulating the Interception of Communications" (the Report).

4. In its Report, LRC concluded that the existing provisions of the Telecommunication Ordinance and Post Office Ordinance in relation to interception of communications did not accord with the requirements of Article 17 of the International Covenant on Civil and Political Rights. Article 17 of the Covenant provides that –

(a) no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; and

(b) everyone has the right to the protection of the law against such interference or attacks.

The provisions in Article 17 are replicated in Article 14 of the Hong Kong Bill of Rights.

5. LRC's main recommendations on regulating interception of communications contained in the Report are as follows –

<u>Proposed offence</u>

(a) it should be an offence intentionally to intercept or interfere with a telecommunication, a sealed postal packet, or a transmission by radio on frequencies which are not licensed for broadcast;

(b) anyone who contravenes the proposed offence should be liable to a fine or a term of imprisonment not exceeding five years or both;

<u>Regulatory framework</u>

(c) a warrant should be required to authorise all interceptions of communications falling within the scope of the proposed offence prohibiting these activities;

(d) all applications for warrants for interception of communications should be made to a judge of the High Court;

(e) a warrant may be issued if the interception is for the purpose of preventing or detecting serious crime, or safeguarding public security of Hong Kong;

(f) a warrant should be issued for an initial period not exceeding 90 days and 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;

(g) where it is impracticable for the Administration or its law enforcement agency to obtain prior authorisation from the court because of the urgency of the situation, the officer proposing to make an interception should, before initiating the interception, obtain authorisation from an officer at the directorate level who is designated for the purpose of giving authorisation in urgent situations;

(h) where an interception is made without the authority of a warrant, an application for a warrant *ex post facto* should be made within 48 hours after the decision to intercept has been made;

Supervisory authority

(i) a supervisory authority should be created to keep the warrant system under review;

(j) a sitting or former judge of the Court of Appeal should be appointed by the Governor, on the recommendation of the Chief Justice, as the supervisory authority;

(k) an aggrieved person who believes that his communications have been unlawfully intercepted may request the supervisory authority to investigate whether there has been a contravention of the statutory requirements relating to the issue of warrants; and

(l) the supervisory authority should furnish annually a public report to the Legislative Council (LegCo).

6. A summary of LRC's recommendations on regulating interception of communications is in **Appendix I**.

White Bill on Interception of Communications Bill

7. In February 1997, the Administration published a White Bill entitled "Interception of Communications Bill" for a one-month consultation. The White Bill sought to regulate and prohibit the interception of communications and to provide for related matters. In its Consultation Paper on the Interception of Communications Bill, the Administration advised that it had accepted the key recommendation of LRC that a judicial warrant system should be introduced to regulate interception of communications. The

Administration had also accepted the recommendation of setting up a Supervisory Authority to review the issue of warrants and to receive complaints from persons regarding unlawful interception by law enforcement agencies.

8. The Administration has so far not introduced the relevant Bill into LegCo. A copy of the Consultation Paper is in **Appendix II**.

The Interception of Communications Ordinance

9. On 28 June 1997, the Interception of Communications Bill, a Member's bill introduced by Hon James TO, was enacted as the Interception of Communications Ordinance (Cap. 532) (IOCO). IOCO provides laws on and in connection with the interception of communications transmitted by post or by means of a telecommunication system and to repeal section 33 of the Telecommunication Ordinance. A copy of IOCO is in **Appendix III** for members' reference. Section 1(2) of IOCO provides that the Ordinance shall come into operation on a day to be appointed by CE. So far CE has not appointed the commencement date.

Implementation of the Interception of Communications Ordinance and review of interception of communications

Council questions raised by Members relating to interception of communications

Council meeting on 30 September 1998

10. At the Council meeting on 30 September 1998, Hon James TO asked an oral question on the commencement date of IOCO. In response, the Administration stated that -

(a) when the Interception of Communications Bill was debated in LegCo in June 1997, the Administration had indicated that it was strongly opposed to the passage of the Bill. The legislative proposals were drawn up without prior consultation with the law enforcement agencies. The implementation of IOCO could seriously jeopardise law enforcement agencies' capability to combat serious crimes and safeguard the security of Hong Kong. The Administration was assessing the impact that IOCO could bring to law enforcement work and therefore had not appointed a commencement date for IOCO;

(b) the Administration was pressing ahead with a thorough review of the whole issue of regulation of interception of communications taking into account comments received from the public

consultation on the White Bill on Interception of Communications, the changes introduced by IOCO and the law enforcement problems arising from IOCO. As the issue was still under review, the Administration did not yet have any plan to promulgate the commencement date of IOCO; and

(c) the key principle adopted by the Administration was that an ordinance would be brought into operation when it was in the interest of the community to do so.

11. The question and the reply are available at http://www.legco.gov.hk/yr98-99/english/counmtg/hansard/980930fe.htm.

Council meeting on 10 November 1999

12. At the Council meeting on 10 November 1999, Hon James TO asked an oral question on the implementation of IOCO and the recommendations in the report entitled "Privacy : Regulating the Interception of Communications" published by LRC in December 1996.

13. In response, the Administration made the following points -

(a) since the Bill was passed by LegCo, the Administration had been conducting a comprehensive review on interception of communications. The review included researching and evaluating the legislation and operational practices of other countries in this area, assessing public views received from the public consultation on the White Bill on Interception of Communications as well as changes introduced by IOCO and the enforcement problems arising from it;

(b) as issues relating to interception of communications were highly complicated, it was difficult to commit a firm timetable for completing the review at that point in time but it would endeavour to proceed with the task as quickly as practicable; and

(c) the review of interception of communications would include consideration of the recommendations of LRC. Until the review had been completed, the Administration could not confirm the elements of the future system regulating the interception of communications. While the Administration did not rule out the adoption of any of the LRC's recommendations, it was premature to confirm whether any particular recommendation would be adopted.

14. The question and the reply are available at http://www.legco.gov.hk/yr99-00/english/ counmtg/hansard/991110fe.pdf.

Deliberations of the Panel on Security

15. At its meetings on 2 April and 10 June 2004, the Panel on Security discussed the review undertaken by the Administration on interception of communications. Members expressed concern that IOCO had not yet been brought into operation.

16. The Administration responded that the implementation of IOCO in its current form would pose serious operational difficulties to law enforcement agencies and prejudice the security of Hong Kong. In view of this, the Chief Executive in Council decided on 8 July 1997 that IOCO should not be brought into operation pending a review. The Administration had set up an interdepartmental working group in late 1999 to undertake a comprehensive review of the existing law, regulatory regime and related matters in relation to interception of communications. As part of the review, the working group examined the relevant legislation and regulatory framework in other jurisdictions. The working group would also take into account the significant legislative amendments that had been introduced in other jurisdictions since the "911" incident in the United States. The Administration assured members that the Panel would be consulted on the way forward after the review was completed.

17. The Panel had asked the Administration to explain the difficulties encountered in the review of IOCO and to provide the timetable for completion of the review. The Administration assured members that it has no intention to delay indefinitely the review of the matter. The Administration advised the Panel that the review had taken longer than anticipated as it covered highly technical and complex issues. In addition, the rapid development of communications technologies had compounded the complexity of the task. In drawing up its recommendations, the working group would strike a balance between the need to provide sufficient powers to law enforcement agencies and to protect the rights of individuals and their personal privacy. The Administration would make every effort to submit its policy recommendations to the Panel during the 2004-05 session.

Research study on the regulation of interception of communications

18. The Panel had asked the Research and Library Services Division of the LegCo Secretariat to conduct a research study on the regulation of interception of communications in overseas jurisdictions. The research report, which studies the statutory regulatory regimes of interception of communications in the United Kingdom (UK), the United States (US) and Australia, was presented

to the Panel at its meeting on 1 March 2005. The report (RP02/04-05) also provides a comparison of the warrant systems for interception of communications in the Hong Kong Special Administrative Region, UK, US and Australia. The relevant extract from the report is in **Appendix IV** for members' easy reference.

Regulation of surveillance

District Court rulings

19. In Criminal Case No. DCCC689 of 2004, the District Court was ruling on admissibility of recordings obtained by covert surveillance into evidence. The judge found that there was no legislative framework in Hong Kong to regulate covert surveillance, and thus the minimum degree of legal protection to which Hong Kong citizens are entitled under Article 30 of the Basic Law was lacking. The judge concluded that the system of covertly intercepting private communications as practised by ICAC in the case was not "in accordance with legal procedures", and the recordings were made in breach of Article 30 and so were unlawfully made. The judge remarked, however, that a defendant is not entitled to have the unlawfully obtained evidence excluded simply because it has been so obtained. What he is entitled to is an opportunity to challenge its use and admission into evidence, and a judicial assessment of the effect of the admission upon the fairness of the trial. As the judge could not find any unfairness in admitting the recordings into evidence despite they are unlawfully obtained, he admitted them into evidence.

20. In Criminal Case No. DCCC687 of 2004, the District Court again considered covert surveillance by ICAC in an application for permanent stay of the proceedings. The judge found that ICAC deliberately and intentionally recorded a conversation knowing that legal advice would almost certainly be given. The judge also found that it was not a situation where ICAC came into possession of privileged material by mistake or accident or only where privileged conversations might have taken place. That was held to be a breach of a fundamental condition upon which the administration of justice as a whole rests. The judge thus ordered a permanent stay.

21. At its meeting on 22 July 2005, the Panel on Security discussed the circumstances surrounding the resignation of the Director of Investigation (Government Sector) of the Operations Department of ICAC. Some members referred to the District Court's ruling in paragraph 20 above and queried whether ICAC had frequently monitored communication between suspects and their lawyers. ICAC responded that –

(a) covert surveillance had regularly been used in the past in ICAC's investigation of corruption. Evidence gathered through such

means had been produced in prosecutions and accepted as evidence by the court; and

(b) there was no question of ICAC frequently monitoring communication between suspects and their lawyers. Only in very exceptional circumstances where there were strong reasons to suspect that a lawyer was a party to corruption or related crime would ICAC consider monitoring the communication between a suspect and his lawyer. At all such times, such action would be taken in accordance with the law.

Review of regulation of surveillance

22. The two District Court rulings have given rise to wide public concern about how law enforcement agencies carry out covert surveillance in the course of their work. In its paper entitled "Surveillance by Law Enforcement Agencies" for the Panel on Security (issued to members on 18 July 2005), the Administration informed the Panel that it has been reviewing the matter with a view to formulating a way forward, and is actively considering what should be done to provide a clearer legal basis for surveillance operations by law enforcement agencies.

23. According to the Administration, LRC has set up a Privacy Sub-committee to look into various privacy-related issues, including surveillance by both public entities (law enforcement agencies) as well as private parties (such as the media and private detectives). LRC is still continuing its deliberations on the subject.

Law Enforcement (Covert Surveillance Procedures) Order

24. Made by the Chief Executive on 30 July 2005 under Article 48(4) of the Basic Law, the Law Enforcement (Covert Surveillance Procedures) Order (the Order) was published in the Gazette on 5 August 2005. The Order, which regulates covert surveillance activities undertaken by law enforcement agencies, came into operation on 6 August 2005.

25. A comparison of provisions governing authorisation to carry out interception of communications or covert surveillance in the Telecommunications Ordinance, IOCO and the Order prepared by the Legal Service Division is in LC Paper No. LS103/04-05.

Relevant papers

26. For details of the discussions, members may wish to refer to the following documents –

Minutes

(a) minutes of the meeting of the Panel on Security on 2 April 2004 (LC Paper No. CB(2)2276/03-04) issued vide LC Paper No. CB(2)2277/03-04 on 11 May 2004;

(b) minutes of the meeting of the Panel on Security on 10 June 2004 (LC Paper No. CB(2)3183/03-04) issued vide LC Paper No. CB(2)3184/03-04 on 30 July 2004;

(c) minutes of the meeting of the Panel on Security on 1 March 2005 (LC Paper No. CB(2)1392/04-05) issued vide LC Paper No. CB(2)1393/04-05 on 27 April 2005;

Papers

(d) Administration's paper entitled "Review on Interception of Communications" for the meeting of the Panel on Security on 2 April 2004 (LC Paper No. CB(2)1873/03-04(04)) issued vide LC Paper No. CB(2)1899/03-04 on 30 March 2004;

(e) Secretary for Security's speaking note regarding progress of review of interception of communication at the meeting of the Panel on Security on 10 June 2004 (LC Paper No. CB(2)2749/03-04(01)) issued vide LC Paper No. CB(2)2749/03-04 on 11 June 2004;

(f) research report entitled "Regulation of Interception of Communications in Selected Jurisdictions" (RP02/04-05) prepared by the Research and Library Services Division of the LegCo Secretariat issued vide LC Paper No. CB(2)836/04-05 on 7 February 2005;

(g) judgment delivered by the District Court on 22 April 2005 issued vide LC Paper CB(2)1420/04-05 on 29 April 2005;

(h) judgment delivered by the District Court on 5 July 2005 issued vide LC Paper CB(2)2280/04-05 on 14 July 2005; and

(i) Administration's paper entitled "Surveillance by Law Enforcement Agencies" (LC Paper No. CB(2)2315/04-05(01)) issued vide LC Paper No. CB(2)2315/04-05 on 18 July 2005.

27. The above papers are available on the website of LegCo (http://www.legco.gov.hk).

Council Business Division 2
Legislative Council Secretariat
12 August 2005

Appendix I

The Law Reform Commission's recommendations on regulating the interception of communications

The proposed offence

1. It should be an offence intentionally to intercept or interfere with -

   (a) a telecommunication;

   (b) a sealed postal packet; or

   (c) a transmission by radio on frequencies which are not licensed for broadcast,

while the telecommunication, postal packet or radio transmission is in the course of transmission.

2. "Interference" for the purposes of the proposed offence should include destruction, corruption or diversion.

3. Anyone who contravenes the proposed offence should be liable to a fine or a term of imprisonment not exceeding five years or both.

4. A person should not be guilty of the proposed offence if -

   (a) one of the parties to the communication has consented to the interception;

   (b) the communication is intercepted for purposes connected with the prevention or detection of radio interference or for ensuring compliance with a licence issued under the Telecommunication Ordinance; or

   (c) the communication is intercepted for purposes connected with the provision of telecommunication service or with the enforcement of any enactment relating to the use of that service.

5. The Telecommunications Authority should specify in the licences granted under the Telecommunication Ordinance the circumstances under which and the extent to which interceptions for operational purposes may be carried out. Such terms and conditions should also be made available to the public for inspection.

The regulatory framework

(A) The warrant system

6. A warrant should be required to authorise all interceptions of communications falling within the scope of the proposed offence prohibiting these activities.

7. All applications for warrants for interception of communications should be made to a judge of the High Court.

8. The Postmaster General should have a power to delay a postal packet for such time as may reasonably be necessary for the purpose of obtaining a warrant authorising him to intercept postal packets.

(B) Grounds on which a warrant may be issued

9. A warrant may be issued if the interception is for the purpose of –

(a) preventing or detecting serious crime; "serious crime" should be defined by virtue of the maximum sentence applicable to the offence. The appropriate level of sentence should be determined by the Administration, but account should be taken of the need to provide a lower sentencing threshold for offences involving an element of bribery or corruption;

(b) safeguarding public security in respect of Hong Kong.

(C) No application by the private sector

10. Only the Administration and its law enforcement agencies may apply for a warrant authorising interception of communications. The application should be made by a senior officer but it should be a matter for the Administration to decide which of its post-holders should be authorised to apply for a warrant.

(D) Form of application

11. An application for a warrant authorising interception of communications should be made in writing.

(E) Matters on which judge must be satisfied

12. A warrant authorising interception of communications should be issued only if the judge is satisfied that -

(a) there is reasonable suspicion that an individual is committing, has committed or is about to commit a serious crime, or, as the case may be, the information to be obtained is likely to be of substantial value in safeguarding public security in respect of Hong Kong;

(b) there is reasonable relief that information relevant to the investigation will be obtained through the interception; and

(c) the information to be obtained cannot reasonably be obtained by less intrusive means.

13. In reaching a conclusion on the appropriateness of issuing a warrant, the judge should have regard to the following factors –

(a) the immediacy and gravity of the crime or the threat to public security in respect of Hong Kong, as the case may be;

(b) the likelihood of the crime or threat occurring; and

(c) the likelihood of obtaining the relevant information by the proposed interception.

(F) Information to be provided on application for a warrant

14. An application for a warrant authorising interception of communications should be accompanied by an affidavit. The information to be provided in the affidavit should include –

(a) the name, identity card number and rank or post of the person making the application;

(b) the facts relied upon to justify the belief that a warrant should be issued, including the particulars of the serious crime or the threat to public security in respect of Hong Kong;

(c) the identity of the person, if known, whose communications are to be intercepted;

(d) a general description of the form of communications to be intercepted and the manner of interception proposed to be used;

(e) the nature and location of the facilities from which the communication is to be intercepted, if applicable;

(f) the nature and location of the place, if known, at which communications are to be intercepted;

(g) the number of instances, if any, on which an application has been made in relation to the same subject matter or the same person and whether that previous application was rejected or withdrawn;

(h) the period for which the authorisation is requested; and

(i) whether other less intrusive means have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or whether the matter is so urgent that less intrusive means cannot be tried.

(G) Duration and renewal of warrant

15. A warrant should be issued for an initial period not exceeding 90 days and 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.

16. An application for renewal of a warrant should be accompanied by an affidavit which includes the following matters –

(a) the reason and period for which the renewal is required;

(b) particulars about the interceptions already made under the warrant and an indication of the nature of information obtained by such interceptions; and

(c) (i) the number of instances on which an application for renewal had been made in relation to the same warrant or the same target and whether the previous application was withdrawn, denied or approved,

(ii) the date on which each application was made, and

(iii) the name of the judge to whom each such application was made.

(H) Entry on to premises to effect interceptions

17. An application for a warrant authorising interception of communications may include a request that the warrant authorise entry on to premises for the purposes of the interception but not otherwise.

(I) Content of warrant

18. The warrant authorising interception of communications should be specific as to –

(a) the object or objects of the proposed interception;

(b) the type of communications to be intercepted; and

(c) the method by which the communications are to be intercepted.

19. The authorising judge may impose such other restrictions or conditions as he may consider appropriate.

(J) Ex post facto applications

20. The court may issue a warrant *ex post facto* where there is reasonable cause to believe that –

(a) a warrant would have been granted if the making of an application prior to interception had not been rendered impracticable because of the urgency of the situation; and

(b) a pressing and imminent opportunity to secure information of a significant nature arises in circumstances where the urgency of the situation is such that an application for a warrant prior to interception would be likely to frustrate -

(i) the prevention of serious crime;

(ii) the apprehension of those reasonably suspected to be responsible for a serious crime; or

(iii) the obtaining of information which is likely to be of substantial value in safeguarding public security in respect of Hong Kong.

21. Where an interception is made without the authority of a warrant, an application for subsequent ratification should be made to the court within 48 hours after the decision to intercept has been made.

22. Where it is impracticable for the Administration or its law enforcement agency to obtain prior authorisation from the court because of the urgency of the situation, the officer proposing to make an interception should, before initiating the interception, obtain authorisation from an officer at the directorate level who is designated for the purpose of giving authorisations in urgent situations.

23. Where the directorate officer reasonably believes that the criteria for the issue of a warrant are satisfied and the urgency of the situation necessitates the interception of communications before making an application to the court, he may, on such terms and conditions as he thinks fit, give authorisation to intercept a communication for a period not exceeding 48 hours.

24. An officer who proposes to make an interception without prior authorisation of the court should apply for permission from a directorate officer on every occasion he proposes to do the same. The permission to make an interception must be recorded in writing. Further, its terms and conditions must be specific.

25. In applying for a warrant *ex post facto*, the officer should serve on the court –

(a) an affidavit which includes particulars of the urgent situation because of which the applicant reasonably believed that it was impracticable for him to obtain prior authorisation from the court; and

(b) a copy of the authorisation given by a directorate officer authorising the interception of communications prior to making an application to the court.

26. Where an interception is made without the prior authorisation of the court, the interception should terminate as soon as the purpose is achieved or when the application is denied by the court, whichever is the earlier.

27. Where the *ex post facto* application is denied by the court, the interception should be treated as unauthorised and the material obtained as a result of the interception should be destroyed immediately.

28. Where an *ex post facto* application is denied by a judge, the directorate officer authorising the interception of communications in an urgent situation, or the officer making an interception on authority of a directorate officer, should not be guilty of unlawful interception if the court is satisfied that the officer concerned acted in good faith when authorising or making the interception.

29. An application should be allowed to be made *ex post facto* to ratify an interception which was not covered by an existing warrant because of an honest error committed by the applicant, provided that –

(a) the application is made within 48 hours of the applicant having notice of the error; and

(b) the interception would have been authorised if the applicant had applied for it at the time he made the original application.

The application should be accompanied by an affidavit which includes the particulars of the error committed by the applicant and how and when the error was discovered.

Material obtained from interception of communications

30. On an application for a warrant authorising interception of telecommunications, the authorising judge shall make such arrangements as he considers necessary to ensure that –

(a) the extent to which the intercepted material is disclosed;

(b) the number of persons to whom any of the intercepted material is disclosed;

(c) the extent to which the intercepted material is copied; and

(d) the number of copies made of any of the intercepted material

is limited to the minimum that is necessary for the purpose for which the application was made. A transcript shall be treated as a copy of the intercepted material. This requirement will be satisfied if each copy made of any of the intercepted material is destroyed as soon as its retention is no longer necessary for the specified purpose.

31. 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 fruit of interception but also the manner in which the interception was made.

32. 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.

33. There should be no discretion for the judge to admit material obtained through an interception of telecommunications carried out pursuant to a warrant.

34. Material obtained through an interception of communications transmitted other than by electromagnetic means which was carried out pursuant to a warrant shall be admissible as evidence and may be retained for so long as may reasonably be necessary for the purpose of any criminal proceedings.

35. Material obtained through an unlawful interception of telecommunications shall be inadmissible as evidence regardless of its relevance. This prohibition should cover not only the fruit of interception but also the manner in which the interception was made.

36. Material obtained through an unlawful interception of communications transmitted other than by electromagnetic means shall be admissible as evidence.

37. Material obtained through an interception of communications whether carried out with or without lawful authority shall be admissible in evidence in relation to proceedings for the offence prohibiting interception of communications.

38. Consideration should be given by law enforcement agencies to the destruction of material obtained by an unlawful interception of telecommunications, whether in whole or in part, as soon as the material is not reasonably necessary for the purpose of any investigation or criminal proceedings.

39. It is not necessary to require that the person whose communications have been intercepted be notified of that fact.

<u>Compliance enforcement : supervisory authority and remedies</u>

40. (a) A supervisory authority should be created to keep the warrant system under review.

(b) A sitting or former judge of the Court of Appeal should be appointed by the Governor, on the recommendation of the Chief Justice, as the supervisory authority.

(c) The person appointed as the supervisory authority should hold office for a period of three years and should be eligible for reappointment for a further period of three years.

41. (a) The supervisory authority should have power to examine on his own initiative whether a warrant has been properly issued and whether the terms of a warrant have been properly complied with.

(b) The supervisory authority may -

(i) summon before him any person who is able to give any information relating to his review and examine that person for the purposes of such review;

(ii) administer an oath for the purposes of the examination under (i) above; and

(iii) require any person to furnish to him any information (on oath if necessary) and to produce any document or thing which relates to his review.

(c) The supervisory authority shall apply the principles applied by a court on an application for judicial review in reviewing the issue of warrants.

42. (a) An aggrieved person who believes that his communications have been unlawfully intercepted may request the supervisory authority to investigate whether there has been a contravention of the statutory requirements relating to the issue of warrants.

(b) Where the supervisory authority ascertains that there is a warrant affecting the aggrieved person which is still effective, he shall refer the case to the High Court.

(c) On referral of the case from the supervisory authority, a judge of the High Court (preferably the one who originally issued the warrant) shall review the case and decide whether the warrant has been properly issued and complied with.

(d) The review shall be conducted *ex parte* and the judge may examine any person and require him to furnish any information, document or thing that is relevant to the case.

(e) Where the reviewing judge is satisfied that the warrant has been properly issued and complied with, he shall affirm the warrant and notify the supervisory authority accordingly.

(f) Where the judge concludes that the warrant has been improperly issued or complied with, he shall -

(i) set the warrant aside; and

(ii) unless the intercepted material may be required for the purposes of establishing the illegality of the interception, order the destruction of the intercepted material.

(g) After setting the warrant aside, the judge shall refer the case back to the supervisory authority.

(h) The decision of the judge who reviews the case on referral by the supervisory authority shall be final.

(i) Where the warrant affecting the aggrieved person has expired, the supervisory authority shall review whether the warrant had been properly issued and complied with and will have the same power as a judge in dealing with the intercepted material.

(j) Any decision of the supervisory authority shall be final.

43. (a) Where the reviewing judge has set aside a warrant or the supervisory authority concludes that the warrant had not been properly issued or complied with, the supervisory authority shall notify the aggrieved person that there has been a contravention of the statutory requirements relating to the issue of warrants.

(b) In any other case, the supervisory authority shall refrain from making any comments other than informing the aggrieved person that there has been no contravention of the statutory requirements relating to the issue of warrants.

(c) The supervisory authority should have power to delay notification if he is satisfied that this would seriously hinder existing or future investigation of serious crime or prejudice the security of Hong Kong.

44. (a) The supervisory authority should have power to pay compensation to the aggrieved person out of public funds if the authority concludes that the warrant has been improperly issued or complied with, or if the warrant has been set aside by the reviewing judge.

(b) The aggrieved person should not be allowed to claim damages in court if he has already been awarded compensation by the supervisory authority.

45. Where there is evidence suggesting that a crime has been committed by the applicant in obtaining the warrant or by the person executing the same, the supervisory authority may refer the matter to the Attorney General to consider whether to bring criminal proceedings against the offender.

46. The supervisory authority should furnish annually a public report to the Legislative Council.

47. There should be a statutory requirement that the following matters be covered by the report to be furnished by the supervisory authority –

(a) the number of warrants applied for, withdrawn, rejected, granted as requested and granted subject to modifications;

(b) the average length of warrants and their extensions;

(c) the classes of location of the place at which communications were to be intercepted, e.g. domestic, business etc.;

(d) the types of interception involved, e.g. interception of telecommunications, interception of mail etc.;

(e) the major categories of serious crime involved;

(f) statistics relating to the effectiveness of interception in leading to the arrest and prosecution of those charged with serious crime;

(g) the number of reviews conducted by the supervisory authority in response to a request by an aggrieved person and an overview of such reviews; and

(h) the findings and conclusions of the review conducted by the supervisory authority in respect of the application of the warrant system.

48. The supervisory authority should furnish annually a confidential report to the Governor. The report should cover such matters as are required by the Governor, or considered relevant by the supervisory authority.

49. All licensed telecommunications carriers should be required to furnish quarterly reports to the Telecommunications Authority for onward transmission to the supervisory authority. The quarterly reports should provide information relating to the following matters –

(a) acts done by employees of the licensed carriers to assist the interception of telecommunications under a warrant;

(b) the number of warrants acted on during the reporting period; and

(c) the average length of time during which telecommunications were intercepted under warrants which have expired within the reporting period.

50. The Post Office, the Customs and Excise Service and the courier companies should furnish quarterly reports to the supervisory authority containing the following matters –

(a) acts done by their employees to assist the interception of postal mail under a warrant;

(b) the number of warrants acted on during the reporting period; and

(c) the total number of items intercepted.

51. Any person who intercepts a communication unlawfully should be liable to pay compensation to the person who suffers damage by reason of the unlawful interception unless the latter has been awarded compensation by the supervisory authority. Damage should be defined as including injury to feelings.

52. The remedy to be granted by a court in a civil action for unlawful interception may include an order requiring the defendant to pay punitive damages to the aggrieved party.

CONSULTATION PAPER

ON

INTERCEPTION OF COMMUNICATIONS BILL

February 1997
Security Branch

Content

SECTION I

EXPLANATORY NOTES ON THE

INTERCEPTION OF COMMUNICATIONS BILL

EXPLANATORY NOTES ON THE

INTERCEPTION OF COMMUNICATIONS BILL

INTRODUCTION

Members of the public are invited to comment on the Interception of Communications Bill in Appendix A by 4 April 1997.

2. Submissions should be addressed to -

Secretary for Security
Government Secretariat
6th Floor, Central Government Offices (Main Wing)
Lower Albert Road
Hong Kong

BACKGROUND

3. In December 1996, the Law Reform Commission (LRC) published a report entitled "Privacy: Regulating the Interception of Communications" (the Report). The key recommendation is that a judicial warrant system should be introduced to regulate interception of communications and replace the current arrangement of executive warrants under Section 33 of the Telecommunication Ordinance and Section 13 of the Post Office Ordinance (Appendix B).

4. The LRC considers that the existing provisions under both Ordinances are not clear enough on the conditions on which interceptions may be authorized. They do not provide sufficient protection against unlawful or arbitrary interference with the individual's right to privacy and freedom of communication as provided in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). It should be noted also that Article 30 of the Basic Law (BL) provides that the freedom and privacy of communication of Hong Kong residents shall be protected by law, and that there should be no infringement except in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.

5. We have accepted the key recommendation of a judicial warrant system, and propose that the grounds for applying a warrant should be the prevention and detection of serious crime or safeguarding the security of Hong Kong. We have also accepted the recommendation of setting up a Supervisory Authority to receive complaints from persons regarding unlawful interception by law enforcement agencies.

6. However, given the complexities of the issue and its wide-ranging implications, we believe that there is a need to consult interested parties of the community. We consider the publication of a White Bill is the best means to gauge public opinion over this issue. A careful assessment of public opinion, obtained through consultation and analysis, should help the Government understand the likely reaction of the community to any proposed course of action or change in policy.

Scope of our Proposals

7. We have examined the 64 recommendations in the Report. We accept 14 in full, 22 in principle or with adaptations to suit law enforcement practice, and rejected 8. The remaining 20 are either not directly relevant to our proposed regulatory framework or require further consideration.

8. In our proposals, communications by post refers to those sent via the Post Office and do not include couriers which are not covered by Section 13 of the Post Office Ordinance. We feel that it would be too complicated to bring couriers, which are not well defined in the law, under our proposed regime. As regards communications by telecommunication, they cover all forms of telecommunications including telephone calls (via fixed and mobile phones), facsimile messages, telegrams, pagers and radiocommunication messages in real time transmission, i.e. "in the course of its sending".

9. Communications transmitted via the computer network are not covered in this Bill. Section 27A of the Telecommunication Ordinance was enacted to form part of the Computer Crimes Ordinance in 1993 to prohibit unauthorised access to computer by telecommunication. We therefore consider that this area of communication has been sufficiently protected.

10. We propose that -

Offences and Exemptions (clauses 3 and 4)

(a) it should be an offence, punishable by imprisonment of two years and a fine at level 5 ($50,000), to intercept a communication intentionally in the course of its sending by post or by telecommunication, unless such action is pursuant to a judicial warrant or exempted in the Bill;

(b) the following should be exempted from the offence provision described in (a):-

i) interception by law enforcement agencies of radiocommunications for which it is impossible to specify the target and the radio spectrum used by criminals, for example, smugglers using unlicensed telecommunication equipment;

ii) activities which may constitute interception of communications but are already governed by existing legislation, for example, examination of postal packet under the Import and Export Ordinance to detect contraband;

iii) interception involving one-party consent, for example, in a kidnapping case, the victim's family may consent to interception by Police; and

iv) assistance and support provided by carriers to Government to effect a warrant;

Warrant System (clauses 5-9)

(c) an authorized public officer may apply to one of three designated High Court judges for the issue of a warrant authorizing interception of communications where the information required cannot reasonably be obtained by other means and is for the purpose of -

i) preventing, investigating or detecting serious crime i.e. offences carrying a maximum imprisonment term of not less than seven years; or

ii) the security of Hong Kong;

(d) where it is impracticable to obtain a warrant because of the urgency of the situation, for example, life is at risk, it should be permissible to apply *ex post facto* for a warrant not later than two working days after the interception;

(e) a warrant should be issued for an initial period not exceeding six months, and there should be no upper limit on the number of renewals made;

Safeguards (clause 10)

(f) authorized public officers should be required to devise administrative arrangements to limit:

i) the extent to which intercepted material is disclosed;

ii) the number of persons to whom any of the intercepted material is disclosed;

iii) the extent to which the intercepted material is copied; and

iv) the number of copies made of any of the material.

The intercepted material and any copies made of it should be destroyed as soon as their retention is no longer necessary for any of the specified purposes;

Non-admissibility of Intercepted Materials in Evidence (clause 11)

(g) intercepted materials should not be admissible as evidence in the court to avoid revealing our law enforcement capabilities. Exception should be made where the intercepted materials are used to prove an illegal interception. In line with existing practice, intercepted materials which are physical items and which can be used to prove a criminal offence, for example, a postal article should also be admissible as evidence;

Supervisory Authority (clauses 12-14)

(h) a Justice of Appeal should be appointed by the Governor, from amongst nominations submitted to him by the Chief Justice, as a "Supervisory Authority" to review the issue of and compliance with

warrants and the adequacy of arrangements made under (f) above. The Authority will also be empowered to receive and examine complaints from persons who believe that their communications have been intercepted and award compensation out of public funds if a contravention is found to have occurred. To promote accountability, it should furnish annually a report to the Governor and the Legislative Council covering the number of warrants authorized and their average length and extensions.

The White Bill

11. **Clause 3** prohibits the interception of communications and sets out exemptions. It also makes provisions requiring carriers and the Postmaster General to provide assistance in connection with the interception of telecommunications and postal articles respectively pursuant to the Governor's written direction.

12. **Clause 4** prohibits the disclosure of intercepted messages and information on the use of telecommunication services subject to certain exceptions.

13. **Clauses 5 and 6** provide for the issue of warrants by designated judges to authorized public officers for interception of communications on specified grounds, where the information sought cannot reasonably be acquired by other means. For postal articles, the judge may authorize their seizure if it is of value to the investigation of serious crime, and such articles should be admissible in evidence.

14. **Clause 7** permits an authorized public officer to carry out an interception without a warrant under certain conditions, but requires an application for a warrant be made within 2 working days of the interception and the destruction of the intercepted material if the application is refused.

15. **Clause 8** specifies that a warrant can be issued only for a maximum period of 6 months, and permits successive renewals of the warrant for the same duration.

16. **Clause 9** empowers the Chief Justice to designate not more than three High Court Judges at any time for the issue of warrants.

17. **Clause 10** requires authorized public officers to make safeguards arrangements in relation to intercepted materials.

18. **Clause 11** provides that intercepted materials under clauses 6 and 7 (other then a postal article expressly authorized to be seized), and materials obtained by unlawful interception, should be inadmissible in evidence and should not be made available to any party in any proceeding, except for the proof of certain specified offences concerning unlawful interception.

19. **Clauses 12, 13 and 14** provide for the establishment of a Supervisory Authority and set out its functions and powers.

20. **Clause 15 and Schedule 1** provide for procedural matters before a judge regarding the application and renewal of warrants, and those before the supervisory authority in the case of complaints.

21. **Clause 16** provides for consequential amendments to, in particular, the Post Office Ordinance and the Telecommunication Ordinance.

PUBLIC VIEWS SOUGHT

22. Members of the public are invited to comment on all aspects of the Bill, particularly -

(a) whether it should be introduced to regulate the interception of communications in Hong Kong;

(b) whether the proposed warrant system in Part III is supported;

(c) whether the offences and exemptions in Part II are appropriate;

(d) whether the proposed safeguards in Part IV are supported;

(e) whether the appointment and functions of the Supervisory Authority in Part V are supported; and

(f) the miscellaneous and procedural matters in Part VI.

SECTION II

Appendices

Appendix A : **Interception of Communications Bill**

Appendix B : **Section 33 of the Telecommunication Ordinance**

Section 13 of the Post Office Ordinance

INTERCEPTION OF COMMUNICATIONS BILL

CONTENTS

Clause Page

PART VI

MISCELLANEOUS

A BILL

To

Regulate and prohibit the interception of communications and to provide for related matters.

Enacted by the Governor of Hong Kong, with the advice and consent of the Legislative Council thereof.

PART I

PRELIMINARY

1. Short title and commencement

(1) This Ordinance may be cited as the Interception of Communications Ordinance.

(2) This Ordinance shall come into operation on a day to be appointed by the Secretary for Security by notice in the Gazette.

2. Interpretation

In this Ordinance, unless the context otherwise requires—

"application" (申請) means an application in writing;

"Authority" (監督) means the Supervisory Authority established under section 12(1);

"authorized public officer" (獲授權公職人員) means a public officer authorized under section 5;

"carrier" (傳送者) means a provider of a telecommunication service and includes the agents of the carrier;

"communication" (通訊) means the contents of a communication sent from a sender to a receiver by post or by telecommunication, but does not include the telephone number dialled, the address of the communication, any record maintained by the operator of the system by which the

communication was sent or a communication sent through a computer network;

"copy" (複本), in relation to intercepted material, means a copy, extract or summary of the material, whether or not in documentary form;

"designated judge" (指定法官) means a judge designated under section 9;

"intercept" (截取) means the act of interception by a person other than the person to whom the communication is addressed or that last-mentioned person's agent, and includes—

(*a*) for a postal article, to inspect it prior to its delivery at the address specified on or in relation to the postal article; and

(*b*) for a communication sent by telecommunication, to record, listen to, view or monitor the communication during its sending;

"intercepted material" (被截取的材料) means the communication intercepted pursuant to a warrant and includes any copies, transcripts or records made of the communication;

"judge" (法官) means a designated judge;

"serious crime" (嚴重罪行) means any offence punishable by a maximum period of imprisonment of not less than 7 years;

"telecommunication service" (電訊服務) means the provision of facilities for use by members of the public or by any person for the sending or reception of messages by telecommunication;

"warrant" (手令) means a warrant issued under section 6 or 7.

PART II

PROHIBITION ON INTERCEPTION AND DISCLOSURE

3. Interception

(1) A person who intentionally intercepts a communication in the course of its sending by post or by telecommunication commits an offence and is liable on conviction to a fine at level 5 and to imprisonment for 2 years.

(2) Subsection (1) shall not apply to the interception of a communication—

(*a*) pursuant to a warrant;

(*b*) that is sent by radiocommunication (other than the radiocommunication part of a fixed telecommunication network licensed or exempted under the Telecommunication Ordinance (Cap. 106)) and that is intercepted by a law enforcement agency of the Government for the purpose of preventing, investigating or detecting crime or for the security of Hong Kong;

(*c*) permitted under section 7;

(*d*) for a purpose connected with the establishment, maintenance or provision of postal or telecommunication services under the Post Office Ordinance (Cap. 98) or the Telecommunication Ordinance (Cap. 106) or with the enforcement under, or of the provisions of, an enactment relating to those services;

(*e*) being the examination of any postal packet under section 20(1)(*f*) or 35(3) of the Import and Export Ordinance (Cap. 60);

(*f*) being the re-direction, sending or delivery of any matter pursuant to an order under section 28 of the Bankruptcy Ordinance (Cap. 6);

(*g*) being any interception to which a party to the communication has consented or to which the person who intercepts reasonably believes that such a party has consented;

(*h*) being assistance or support provided by a carrier or an employee of a carrier to the Government in connection with an interception authorized under this Ordinance; or

(*i*) being any interception made pursuant to an Aviation Security Programme drawn up under section 27(1) of the Aviation Security Ordinance (52 of 1996).

(3) The Postmaster General and his agents shall give such assistance in connection with the interception of postal articles under this Ordinance as the Governor directs in writing.

(4) A carrier shall give such assistance in connection with the interception of telecommunications under this Ordinance as the Governor directs in writing.

(5) A carrier who fails to comply with a direction of the Governor under subsection (4) commits an offence and is liable on conviction to a fine at level 5.

(6) The time limited for making a complaint in respect of an offence against subsection (1) or (5) is 3 years from the time when the matter of the complaint arose.

4. Prohibition on disclosure of intercepted messages

(1) A specified person who otherwise than in the course of his duty discloses to any person—

(*a*) the contents of any message which has been intercepted; or

(*b*) any information obtained in connection with an interception concerning details of the use made of telecommunication services provided for any other person by a carrier without the consent of the other person,

commits an offence and is liable on conviction to a fine at level 5 and to imprisonment for 2 years.

(2) A person (other than a specified person) who—

(*a*) discloses to any person—

(i) the contents of any message which has been intercepted; or

(ii) any information obtained in connection with an interception concerning details of the use made of telecommunication services provided for any other person by a carrier without the consent of the other person; and

(*b*) knows or has reasonable grounds to believe that—

(i) where paragraph (*a*)(i) is applicable, the message has been intercepted;

(ii) where paragraph (*a*)(ii) is applicable, the information has been obtained in connection with an interception,

commits an offence and is liable on conviction to a fine at level 5 and to imprisonment for 2 years.

(3) Subsection (1) or (2) shall not apply to a disclosure—

(*a*) which is made for preventing, investigating or detecting crime;

(*b*) which falls within subsection (1)(*a*) or (2)(*a*) and which is made in relation to the execution of a warrant; or

(*c*) which falls within subsection (1)(*b*) or (2)(*b*) and which is made in the interests of the security of Hong Kong or pursuant to an order of court.

(4) In this section, "specified person" (指明人士) means—

(*a*) a carrier;

(*b*) an employee of a carrier; or

(*c*) a person belonging to a class of persons declared under subsection (5) to be a class of persons for the purposes of this definition.

(5) The Secretary for Security may, by notice in the Gazette, declare a class of persons specified in the notice to be a class of persons for the purposes of the definition of "specified person".

(6) A notice under subsection (5) is subsidiary legislation.

PART III

WARRANTS

5. Authorized public officers

The Governor may authorize a public officer of not less than directorate rank or equivalent to apply to a judge for a warrant.

6. Warrants for interception

(1) A judge may issue a warrant authorizing the interception of—

(*a*) such communications as are sent to or from one or more addresses specified in the warrant, being an address or addresses likely to be used for the transmission of communications to or from—

(i) one particular person specified or described in the warrant; or

(ii) one particular set of premises so specified or described; and

(*b*) such other communications (if any) as it is necessary to intercept in order to intercept communications falling within paragraph (*a*).

(2) A warrant may be issued only on application by an authorized public officer and only for a purpose specified in subsection (4).

(3) A judge shall not issue a warrant unless he is satisfied that the information which is sought to be acquired by executing the warrant cannot reasonably be acquired by other means.

(4) A judge may issue a warrant for one or more of the following purposes, but no other—

(*a*) for preventing, investigating or detecting serious crime where there is reasonable cause to believe that the interception is likely to uncover useful information leading (whether by itself or together with anything else) to a suspect or an arrest in respect of serious crime; or

(*b*) for the security of Hong Kong where the interception of communication is likely to be of substantial value in furthering the purpose.

(5) In issuing a warrant for a postal article, a judge may authorize the seizure of the postal article, on the application of an authorized public officer, on being satisfied, on the basis of information provided by the authorized public officer, that there is a reasonable cause to believe that the postal article is of value to the investigation of serious crime that has been committed or that is reasonably suspected of having been or is about to be or is intended to be committed.

7. Application for warrant after interception

(1) Where an authorized public officer—

(*a*) is unable to apply under section 6 for a warrant, because of the urgency of the situation; and

(*b*) believes on reasonable grounds that an interception is immediately necessary to detect or investigate serious crime or prevent its occurrence,

he may authorize in writing a person to carry out the interception without a warrant or carry out the interception himself.

(2) Where an interception takes place under subsection (1), an authorized public officer shall within 2 working days of the interception, apply to a judge for a warrant for the interception.

(3) If an application under subsection (2) is refused, the authorized public officer concerned shall as soon as practicable stop the interception and destroy the intercepted material (if any).

8. Duration and renewal of warrants

(1) A warrant ceases to have effect at the expiry of 6 months from its issue.

(2) An authorized public officer may apply to a judge for the renewal of an initial warrant or a warrant renewed under this section, before its expiration.

(3) The judge may renew the warrant for a further period not exceeding 6 months if he is satisfied that the grounds on which it was issued still exist.

PART IV

SAFEGUARDS FOR INTERCEPTED MATERIAL

9. Designated judges

(1) The Chief Justice may designate a High Court judge to issue warrants.

(2) The number of designated judges shall not exceed 3 at any time.

(3) A warrant may be issued only by a designated judge.

10. Safeguards

An authorized public officer shall make arrangements to ensure that the following requirements are satisfied—

(*a*) that the following are limited to the minimum that is necessary having regard to the purposes specified in section 6(4)—

(i) the extent to which the intercepted material is disclosed;

(ii) the number of persons to whom any of the intercepted material is disclosed;

(iii) the extent to which the intercepted material is copied; and

(iv) the number of copies made of any of the intercepted material; and

(*b*) the intercepted material is destroyed (or, in the case of a postal article, otherwise disposed of) as soon as its retention is not necessary for any of those purposes, including any criminal proceedings arising from any of those purposes.

11. Non-admissibility of intercepted material

(1) Intercepted material and information obtained by interception under section 6 or 7 or unlawful interception (other than a postal article expressly authorized under section 6(5) to be seized under a warrant) shall not be admissible in evidence in any proceedings before a court or tribunal other than to prove that an offence under section 3(1) or 4(1)(*a*) or (2)(*a*)(i), or section 24(*c*) or (*d*) of the Telecommunication Ordinance (Cap. 106), has been committed.

(2) Any intercepted material and any particulars as to an interception (other than a postal article expressly authorized under section 6(5) to be seized under a warrant) shall not be made available to any party to any proceedings, including the prosecution in any criminal proceedings.

(3) In any proceedings before any court or tribunal—

(*a*) evidence which tends to suggest that a warrant has been or is to be issued to an authorized public officer (other than a warrant expressly authorizing a postal article to be seized under section 6(5)) shall not be adduced; and

(*b*) a question which tends to suggest that a warrant (other than a warrant expressly authorizing a postal article to be seized under section 6(5)) has been issued shall not be asked.

(4) This section shall not be construed to preclude the admissibility in evidence of any intercepted material which is—

(*a*) an item the possession, custody or control of which is an offence; or

(*b*) a postal article seized under a warrant issued on an application under section 6(5).

PART V

APPOINTMENT AND FUNCTIONS OF SUPERVISORY AUTHORITY

12. Supervisory Authority

(1) There is hereby established an authority, to be known as the Supervisory Authority, for the purposes of this Ordinance.

(2) The Governor shall appoint a Justice of Appeal, from amongst nominations submitted to him by the Chief Justice, to be the Authority for 3 years or such lesser period as is specified in the appointment.

(3) The Authority shall—

(*a*) keep under review the issue of warrants and their proper execution;

(*b*) review the adequacy of arrangements made for the purposes of section 10;

(*c*) perform such other functions as are imposed on him under this Ordinance.

(4) A Justice of Appeal whose appointment as the Authority has expired may be reappointed to be the Authority.

13. Examinations by Authority

(1) A person who believes that any communication sent to or by him has been intercepted in the course of its sending by means of the post or telecommunication may apply to the Authority for an examination under this section.

(2) Where the Authority receives an application, he shall, subject to section 15(3), ascertain whether or not—

(*a*) a warrant has been issued in relation to the interception (if any); and

(*b*) any provision of this Ordinance relating to the warrant has been contravened.

(3) If on an examination the Authority, applying the principles applicable by a court on an application for judicial review, concludes that a public officer in the purported exercise of his duties or a Department or other agency of the Government has contravened a provision of this Ordinance, he—

(*a*) shall give notice to the applicant stating that conclusion; and

(*b*) may, if he thinks fit, make an order for one or more of the following purposes—

(i) quashing the relevant warrant;

(ii) directing the destruction of copies of the intercepted material;

(iii) ordering the payment by the Government to the applicant of such sum as is specified in the order, by way of compensation.

(4) A sum ordered as compensation under subsection (3)(*b*)(iii) may include compensation for injury to feelings.

(5) The Authority may award as compensation an amount that he, in his discretion, considers to be appropriate.

(6) Where on an examination, the Authority comes to a conclusion other than that referred to in subsection (3), he shall give notice to the applicant that there has not been any contravention of any provision of this Ordinance.

(7) The Authority, to perform his functions under this Ordinance—

(*a*) has the power to examine any matter in which a warrant has been issued; and

(*b*) has access to any official document relating to the warrant or the application for the warrant, including the material intercepted.

(8) An examination by the Authority shall be carried out in private and counsel and solicitors do not have any right of audience before the Authority, but may appear before him if he thinks fit.

(9) A public officer shall disclose or give to the Authority the documents or information the Authority requires to perform the Authority's functions under this Ordinance.

(10) The Authority—

(*a*) shall perform his functions (except his functions under section 14) in such a way as to secure that no document or information which is disclosed or given to the Authority is disclosed or given to any person (including an applicant under subsection (1)) or an authorized public officer, without the consent of the person who disclosed or gave it to the Authority;

(*b*) shall not give reasons for any decision made by him; and

(*c*) subject to section 15(2), may determine the procedure to be adopted in performing his functions.

(11) The decision of the Authority (including any decision as to its jurisdiction) is not subject to appeal or liable to be questioned in any court.

14. Reports by Authority

(1) The Authority shall report to the Governor as to the number of warrants issued and the duration of a warrant, on an average, and the number of extensions granted during the period reported on.

(2) The report shall be submitted within 3 months of the expiry of each 12 months period occurring after the commencement of this section.

(3) The Governor shall cause a report furnished to him under this section to be laid on the table of the Legislative Council.

PART VI

MISCELLANEOUS

15. Procedural matters, etc.

(1) The provisions of Part 1 of Schedule 1 shall be applicable to and in relation to applications under Part III for—

(*a*) the issue of warrants; and

(*b*) the renewal of initial warrants and warrants renewed under Part III.

(2) The provisions of Part 2 of Schedule 1 shall be applicable to and in relation to applications under section 13 for examinations under that section.

(3) The Authority may refuse to carry out an examination under section 13 in relation to any application under that section which falls within a ground specified in Part 3 of Schedule 1.

(4) The Governor in Council may, by notice in the Gazette, amend Schedule 1.

(5) Without prejudice to the generality of subsection (4), the power under that subsection shall extend generally to regulating procedure before a judge and the Authority.

16. Consequential amendments

The enactments specified in Schedule 2 are amended as set out in that Schedule.

SCHEDULE 1

[s. 15]

PROCEDURE BEFORE JUDGE AND AUTHORITY AND GROUNDS ON WHICH EXAMINATION MAY BE REFUSED

PART 1

PROCEDURE BEFORE JUDGE

PART 2

PROCEDURE BEFORE AUTHORITY

PART 3

GROUNDS ON WHICH AUTHORITY MAY REFUSE TO CARRY OUT EXAMINATION UNDER SECTION 13 OF THIS ORDINANCE

SCHEDULE 2 [s. 16]

CONSEQUENTIAL AMENDMENTS

Post Office Ordinance

1. **Warrant of Chief Secretary for opening and delaying postal packets**

Section 13 of the Post Office Ordinance (Cap. 98) is repealed.

2. **Disposal of postal packets opened under section 10 or 12**

Section 14 is amended by repealing ", 12 or 13" and substituting "or 12".

3. **Extension of sections 12 and 14 to articles not transmissible by post**

Section 15 is amended by repealing ", 13".

Post Office Regulations

4. **Regulation amended**

Regulation 10 of the Post Office Regulations (Cap. 98 sub. leg.) is amended by repealing ", 12, or 13" and substituting "or 12".

Telecommunication Ordinance

5. **Penalty for contravention of order under section 33**

Section 30 of the Telecommunication Ordinance (Cap. 106) is repealed.

6. **Power of Governor to prohibit transmission of messages, etc.**

Section 33 is repealed.

Emergency Powers (Extension and Amendment Incorporation) Ordinance

7. **Compensation (Defence) Regulations**

Regulation 2(1) of the Compensation (Defence) Regulations in the First Schedule to the Emergency Powers (Extension and Amendment Incorporation) Ordinance (Cap. 251) is amended, in the definition of "emergency powers"—

(*a*) in paragraph (*a*), by adding "or" at the end;
(*b*) in paragraph (*b*), by repealing "; or" and substituting a comma;
(*c*) by repealing paragraph (*c*).

Explanatory Memorandum

The object of this Bill is to regulate the interception of communications (which is defined for the purposes of the Bill) by prohibiting interception other than in the circumstances specified in the Bill.

2. Clause 1 enables the Secretary for Security to bring the Bill into force on a date or dates appointed by him.

3. Clause 2 contains the definitions with reference to which the provisions of the Bill are to be interpreted. Under this clause, for the purposes of the Bill—

communication is defined as a message sent by post or by telecommunication;

intercept means the act of interception and includes inspection of postal articles and listening, monitoring, viewing and recording telecommunication messages;

sending by telecommunication does not include sending by computer network.

4. Clause 3 prohibits the interception of any communication while it is being sent, except in the circumstances provided for in the Bill. The prohibition does not apply where the interception is under a warrant under the Bill or for purposes connected with the provision of postal or telecommunication services, examining postal packets pursuant to the Import and Export Ordinance (Cap. 60) or an order under the Bankruptcy Ordinance (Cap. 6) or where a party to the communication has consented to the interception.

5. Clause 4 prohibits a person from disclosing the contents of an intercepted message or information concerning details of the use of the services provided for any other person.

6. Clause 5 empowers the Governor to authorize public officers of not less than directorate rank to apply for warrants under the Bill. Clause 6 empowers a judge designated by the Chief Justice to issue a warrant authorizing interception. It also sets out the only purpose for which a warrant may be issued, being for preventing, investigating or detecting serious crime or for the security of Hong Kong. A judge may issue a warrant only if he is satisfied that the information sought to be acquired cannot reasonably be acquired by other means. For postal articles, the judge may authorize their seizure if the postal article is of value to the investigation of serious crime.

7. Clause 7 permits an authorized public officer to carry out an interception without a warrant if he is unable to apply for a warrant because of the urgency of the situation and he has reasonable grounds to believe that the interception is immediately necessary to, inter alia, prevent serious crime. However, he has to make an application for a warrant within 2 working days of the interception and destroy the intercepted material if the application is refused.

8. Clause 8 states that a warrant can be issued only for a maximum period of 6 months and permits successive renewals of the initial warrant, each for a period not exceeding 6 months.

9. Clause 9 empowers the Chief Justice to designate not more than 3 judges at any time for the purpose of issuing warrants.

10. Clause 10 requires authorized public officers to devise safeguards to ensure that the extent to which and the number of people to whom the intercepted material is disclosed, the number of copies made of it is limited to the minimum that is necessary having regard to the purposes specified in clause 6(4). The intercepted material and copies of it are required to be destroyed or otherwise disposed of as soon as their retention is not necessary for those purposes.

11. Clause 11 provides that any intercepted material or copies of it are inadmissible in proceedings other than to prove the offence of unlawful interception (other than a postal article expressly authorized under clause 6(5) to be seized under a warrant). No intercepted material or record or copy is to be provided to the parties to any proceedings. No evidence may be adduced in any proceedings which suggests that a warrant has been issued to a public officer. However, this clause does not prevent, inter alia, the admissibility of evidence of any intercepted material where the possession of it is an offence.

12. Clause 12 provides for the establishment of the office of a Supervisory Authority (who is to be a Justice of Appeal appointed by the Governor from amongst nominations submitted by the Chief Justice) to review the issue of warrants and the adequacy of the safeguards required under clause 10. Under clause 13 the Authority is given power to examine any complaint by a person that his communications have been intercepted. The Authority has power after examining a complaint to quash the relevant warrant, direct the destruction of the material and order compensation to the complainant. Under this clause the Authority has access to the material and documents relevant to the examination and public officers are placed under a duty to provide him with information.

13. Clause 14 requires the Authority to furnish to the Governor a report containing information on the issue of warrants and their renewal, for every period of 12 months after the commencement of the clause. The Governor is to table the reports in the Legislative Council.

14. Clause 15 and Schedule 1 provide for procedural matters before a judge (in the case of warrants) and the Authority (in the case of complaints). It should also be noted that Part 3 of that Schedule sets out the grounds on which the Authority may refuse to carry out an examination under clause 13.

15. Clause 16 and Schedule 2 provide for consequential amendments to, inter alia, the Post Office Ordinance (Cap. 98), the Telecommunication Ordinance (Cap. 106) and the Emergency Powers (Extension and Amendment Incorporation) Ordinance (Cap. 251).

Telecommunication Ordinance (Cap 106)

33. Power of Governor to prohibit transmission of messages, etc.

Whenever he considers that the public interest so requires, the Governor, or any public officer authorized in that behalf by the Governor either generally or for any particular occasion, may order that any message or any class of messages brought for transmission by telecommunication shall not be transmitted or that any message or any class of messages brought for transmission, or transmitted or received or being transmitted, by telecommunication shall be intercepted or detained or disclosed to the Government or to the public officer specified in the order.

Post Office Ordinance (Cap 98)

13. Warrant of Chief Secretary for opening and delaying postal packets

(1) It shall be lawful for the Chief Secretary to grant a warrant authorizing the Postmaster General, or authorizing any or all the officers of the Post Office, to open and delay any specified postal packet or all postal packets of any specified class or all postal packets whatsoever.

(2) It shall be lawful for the Postmaster General to delay any postal packet for such time as may reasonably be necessary for the purpose of obtaining a warrant under this section.

HONG KONG

ORDINANCE NO. 109 OF 1997

L.S.

I assent.

Christopher PATTEN,
Governor.
29 June 1997

An Ordinance to provide laws on and in connection with the interception of communications transmitted by post or by means of a telecommunication system and to repeal section 33 of the Telecommunication Ordinance.

[ ]

Enacted by the Governor of Hong Kong, with the advice and consent of the Legislative Council thereof.

PART I

PRELIMINARY

1. Short title and commencement

(1) This Ordinance may be cited as the Interception of Communications Ordinance.

(2) This Ordinance shall come into operation on a day to be appointed by the Governor by notice in the Gazette.

2. Interpretation

In this Ordinance, unless the context otherwise requires—

"authorized officer" (獲授權人員) means an officer who has been authorized by a court order to intercept a communication in the course of its transmission by post or by means of telecommunication system through the use of any electro-magnetic, acoustic, mechanical or other device;

"communication" (通訊) means postal or telecommunication;

"electro-magnetic, acoustic, mechanical or other device" (電磁、傳音、機械或其他裝置) means any device or apparatus that is used or is capable of being used to intercept a telecommunication, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;

香 港

1997年第109號條例

公印位置

本人批准。

彭定康，
總督
1997年6月29日

本條例旨在為截取以郵遞或透過電訊系統傳送的通訊提供法律監管，並廢除《電訊條例》第33條。

[ ]

由香港總督參照立法局意見並得該局同意而制定。

第I部

導言

1. 簡稱及生效日期

(1) 本條例可引稱為《截取通訊條例》。

(2) 本條例自總督以憲報公告指定的日期起實施。

2. 釋義

在本條例中，除文意另有所指外——

"人" (person) 包括任何組織及任何團體或個人的組成；

"被截取的材料" (intercepted material) 指以截取方式取得郵遞通訊或透過電訊系統傳送的通訊的內容；

"intercept" (截取) means the aural or other acquisition of the contents of any postal communication, telecommunication, or telecommunication through the use of any electro-magnetic, acoustic, mechanical or other device;

"intercepted material" (被截取的材料) means the contents of any postal communication or telecommunication that has been obtained through interception;

"law enforcement officer" (執法人員) means any police officer and any officer appointed—

(*a*) under the Customs and Excise Service Ordinance (Cap. 342);

(*b*) under section 8 of the Independent Commission Against Corruption Ordinance (Cap. 204);

(*c*) by the Immigration Department; or

(*d*) by the Correctional Services Department;

"person" (人) includes any organization and any association or combination of persons;

"serious crime" (嚴重罪行) means any offence punishable by a maximum period of imprisonment of not less than 7 years;

"telecommunication" (電訊) has the same meanings as in section 2 of the Telecommunication Ordinance (Cap. 106).

PART II

PROHIBITION ON INTERCEPTION OF COMMUNICATIONS

3. Prohibition on interception

(1) Subject to the provisions of this section, a person who intentionally intercepts a communication in the course of its transmission by post or by means of telecommunication system shall be guilty of an offence and liable on summary conviction to a fine at level 4 and to imprisonment for 2 years.

(2) A person shall not be guilty of an offence under this section if—

(*a*) the communication is intercepted pursuant to a court order given under section 4; or

(*b*) that person has reasonable grounds for believing that the person to whom, or by whom the communication is made, has consented to the interception.

(3) A person shall not be guilty of an offence under this section if—

(*a*) the communication is intercepted in accordance with the Post Office Ordinance (Cap. 98); or

(*b*) the communication is intercepted in accordance with the Telecommunication Ordinance (Cap. 106).

"執法人員" (law enforcement officer) 指警員及下列人員——

(*a*) 根據《香港海關條例》(第 342 章) 獲委任；

(*b*) 根據《總督特派廉政專員公署條例》(第 204 章) 第 8 條獲委任；

(*c*) 由入民入境事務處委任；或

(*d*) 由懲教署委任；

"通訊" (communication) 指以郵遞或透過電訊系統傳送的通訊；

"電訊" (telecommunication) 指在《電訊條例》(第 106 章) 第 2 條所指的電訊；

"電磁、傳音、機械或其他裝置" (electro-magnetic, acoustic, mechanical or other device) 指任何用作或可以用作截取通訊的裝置或儀器，但不包括用以改正低於正常聽覺至不高於正常聽覺的助聽器；

"截取" (intercept) 指以聽覺或以電磁、傳音、機械或其他裝置的方法獲得郵遞通訊或透過電訊系統傳送的通訊的內容；

"獲授權人員" (authorized officer) 指獲法庭命令授權的人員，該人員獲授權以任何電磁、傳音、機械或其他裝置截取以郵遞或透過電訊系統傳送的通訊；

"嚴重罪行" (serious crime) 指最高刑罰可被判以不少於 7 年的罪行。

第 II 部

禁止截取通訊

3. 禁止截取

(1) 除本條另有規定外，任何人故意在郵遞通訊、透過電訊系統傳送的通訊過程中截取該通訊，即屬犯罪，一經循簡易程序定罪，可處第 4 級罰款及監禁 2 年。

(2) 任何人根據本條不屬犯罪，如——

(*a*) 是根據第 4 條批准的法令截取通訊；或

(*b*) 該人有合理理由相信接受該通訊的人或發出該通訊的人已同意該截取。

(3) 任何人根據本條不屬犯罪，如——

(*a*) 是根據《郵政署條例》(第 98 章) 截取通訊；或

(*b*) 是根據《電訊條例》(第 106 章) 截取通訊。

(4) In any proceedings against a person for an offence under this section, it shall be a defence to the accused to prove that the interception was conducted in good faith for the purpose of revealing a serious threat to public order or to the health and safety of the public.

PART III

AUTHORIZATION FOR INTERCEPTION OF COMMUNICATIONS

4. Authorization for interception

(1) Subject to the provisions of this section, a judge of the High Court may make a court order authorizing a person named in the court order to intercept, in the course of its transmission by post or by means of a telecommunication system, such communications as are described in the order.

(2) An order shall not be made under this section unless it is necessary—

(*a*) for the purpose of preventing or detecting a serious crime; or

(*b*) in the interest of the security of Hong Kong.

(3) In deciding whether it is necessary to make an order, the judge shall determine that—

(*a*) there are reasonable grounds to believe that an offence is being committed, has been committed or is about to be committed;

(*b*) there are reasonable grounds to believe that information concerning the offence referred to in paragraph (*a*) will be obtained through the interception sought;

(*c*) all other methods of investigation have been tried and have failed, or are unlikely to succeed; and

(*d*) there is good reason to believe that the interception sought will result in a conviction.

5. Application for authorization

(1) An application to the High Court for an order authorizing the interception of communications under section 4 may only be made by—

(*a*) any officer of the Royal Hong Kong Police Force of or above the level of superintendent;

(*b*) any senior officer of the Customs and Excise Service as defined in section 2 of the Customs and Excise Service Ordinance (Cap. 342);

(*c*) any investigating officer authorized by the Commissioner of the Independent Commission Against Corruption and who is appointed under section 8 of the Independent Commission Against Corruption Ordinance (Cap. 204);

(4) 在根據本條對任何人提出起訴的訴訟過程中，被控人可藉證明該截取是真誠地為公開一項對公共秩序或公眾的健康或安全的嚴重威脅而進行，以此作為免責辯護。

第 III 部

授權截取通訊

4. 授權截取

(1) 除這條另有規定外，高等法院的法官可發出法令授權在法令內被指明的任何人對在郵遞通訊或透過電訊系統傳送的通訊過程中截取在法令內被指明的通訊。

(2) 除在以下需要的情況外，否則法院不可根據本條發出法令——

(*a*) 為防止或偵查一項嚴重罪行；或

(*b*) 為香港的安全的利益。

(3) 該法官在決定是否需要發出法令時須裁定——

(*a*) 有合理理由相信有罪行正在進行，已進行或將進行；

(*b*) 有合理理由相信在 (*a*) 段所指的罪行的資料將可從該截取中獲得；

(*c*) 已嘗試其他調查方法並已失敗，或很有可能不會成功；及

(*d*) 有理由相信該截取將導致定罪。

5. 申請授權

(1) 只有下列人士可向高等法院申請法令以進行根據第 4 條授權的截取通訊——

(*a*) 皇家香港警隊警司級或以上的人員；

(*b*) 根據《香港海關條例》(第 342 章) 第 2 條指明的任何海關高級人員；

(*c*) 根據《總督特派廉政專員公署條例》(第 204 章) 第 8 條委任的獲廉政專員授權的任何調查人員；

(*d*) any senior officer of the Immigration Department; or

(*e*) any senior officer of the Correctional Services Department.

(2) An application for authorization shall be made ex parte and in writing to a judge of the High Court in Chambers and shall be accompanied by a sworn affidavit deposing to the following matters—

(*a*) the name and rank of the officer making the application;

(*b*) particulars of the offence or offences under investigation;

(*c*) the name and address of the person who is believed to have committed, is committing or is about to commit the offence or offences under paragraph (*b*) and whose communications are to be intercepted for the purpose of investigating that offence;

(*d*) a description of the nature and location of the facilities from which or the place where the communication is to be intercepted;

(*e*) the type of communication sought to be intercepted and the method of interception to be used;

(*f*) whether he wishes for a person authorized under the Post Office Ordinance (Cap. 98) or the Telecommunication Ordinance (Cap. 106) to assist him with the interception;

(*g*) what other investigative methods have been used and why they have failed or are unlikely to succeed;

(*h*) the duration of the interception; and

(*i*) particulars of any previous application involving the same person.

(3) Where a serious threat of death or bodily harm to a person exists and it is impracticable to make an application for an order authorizing the interception of communications in accordance with subsection (2), an officer listed in subsection (1), with the written permission of—

(*a*) the Commissioner of Police, where the officer involved is an officer of the Royal Hong Kong Police Force;

(*b*) the Commissioner for Customs and Excise Service, where the officer involved is a senior officer of the Customs and Excise Service;

(*c*) the Commissioner of the Independent Commission Against Corruption, where the officer is an officer of the Independent Commission Against Corruption;

(*d*) the Director of Immigration, where the officer is an officer of the Immigration Department; or

(*e*) the Commissioner of Correctional Services, where the officer is an officer of the Correctional Services Department,

may intercept a communication without prior authorization.

(*d*) 人民入境事務處任何高級人員；或

(*e*) 懲教署任何高級人員。

(2) 申請授權可單方面以書面向在內庭的高等法院法官提出，並須附上誓章，述及以下事項——

(*a*) 申請人員的姓名及職級；

(*b*) 在調查中的罪行的詳情；

(*c*) 相信已犯有、正犯有或將犯有 (*b*) 段所述罪行的人的姓名及地址，而截取該人的通訊是為調查該罪行；

(*d*) 被截取通訊的地方或有關設備的地點及性質的描述；

(*e*) 將被截取通訊的形式及使用截取的方法；

(*f*) 申請人是否欲獲得一名根據《郵政署條例》(第 98 章) 或《電訊條例》(第 106 章) 授權的人協助他進行截取；

(*g*) 其他已嘗試的調查方法及其失敗或很有可能不會成功的原因；

(*h*) 截取的期限；及

(*i*) 在任何以前申請中涉及相同人士的詳情。

(3) 凡在出現對死亡或人身傷害有嚴重威脅及不可能根據第 (2) 款申請授權截取通訊的情況，在獲得以下人士的書面批准下，第 (1) 款列明的人員可在未獲得授權下截取通訊——

(*a*) 若涉及皇家警隊人員，由警務處處長批准；

(*b*) 若涉及香港海關的高級人員，由香港海關總監批准；

(*c*) 若涉及總督特派廉政專員公署的人員，由廉政專員批准；

(*d*) 若涉及人民入境事務處的人員，由人民入境事務處處長批准；或

(*e*) 若涉及懲教署的人員，由懲教署署長批准。

(4) Where an interception under subsection (3) occurs, unless the officer conducting the interception makes an application for authorization in accordance with subsections (1) and (2) within 48 hours from the beginning of the interception giving—

(*a*) the reasons for not making an application prior to interception; and

(*b*) a copy of the written permission given by—

(i) the Commissioner of Police, where the officer involved is an officer of the Royal Hong Kong Police Force;

(ii) the Commissioner for Customs and Excise Service, where the officer involved is an officer of the Customs and Excise Service;

(iii) the Commissioner of the Independent Commission Against Corruption, where the officer involved is an officer of the Independent Commission Against Corruption;

(iv) the Director of Immigration, where the officer is an officer of the Immigration Department; or

(v) the Commissioner of Correctional Services, where the officer is an officer of the Correctional Services Department,

the interception shall be deemed unlawful under section 3.

(5) Any interception which is conducted pursuant to subsection (3) shall immediately terminate when the communication sought is obtained or when an application for authorization is denied, whichever is earlier.

(6) Where an application for authorization under subsection (4) is denied, the intercepted material shall be destroyed immediately.

PART IV

THE COURT ORDER

6. Scope of the court order

(1) A court order authorizing the interception of communications, oral or otherwise, pursuant to section 4 shall specify—

(*a*) the name and rank of the authorized officer;

(*b*) the offence or offences in respect of which communications may be intercepted;

(*c*) the name and address of the person whose communications are to be intercepted;

(4) 凡根據第 (3) 款進行截取，除有關人員在開始截取後的 48 小時內，根據第 (1) 及 (2) 款申請授權，並列明——

(*a*) 在截取前未有提出申請的原因；及

(*b*) 下列人士的書面批准的副本——

(i) 若涉及皇家警隊人員，由警務處處長批准；

(ii) 若涉及香港海關的高級人員，由香港海關總監批准；

(iii) 若涉及總督特派廉政專員公署的人員，由廉政專員批准；

(iv) 若涉及人民入境事務處的人員，由人民入境事務處處長批准；或

(v) 若涉及懲教署的人員，由懲教署署長批准，

否則該截取被視為在第 3 條下屬非法。

(5) 任何根據第 (3) 款進行的截取須在已獲得所需要的通訊或申請授權不獲批准時立即停止，而以兩者中較早的日子為準。

(6) 凡根據第 (4) 款申請授權不獲批准時，被截取的材料須被立即毀滅。

第 IV 部

法令

6. 法令的範圍

(1) 根據第 4 條發出授權截取通訊的法令須列明——

(*a*) 獲授權人員的姓名及職級；

(*b*) 與該將被截取通訊有關的罪行；

(*c*) 將被截取通訊的人的姓名及地址；

(*d*) the type of communication that may be intercepted and the method of interception used;
(*e*) whether or not the authorized officer can engage a person authorized under the Post Office Ordinance (Cap. 98) or the Telecommunication Ordinance (Cap. 106) in the course of his duty to assist in the interception;
(*f*) the nature and location of the facilities from which or the place where the communication is to be intercepted;
(*g*) the duration for which the interception is authorized; and
(*h*) subject to section 9, to whom the intercepted material may be disclosed to.

(2) For the purposes of subsection (1)(*h*), a judge shall only authorize that the intercepted material be disclosed to those other law enforcement officers who are involved in the investigation of that offence or those offences specified in subsection (1)(*b*).

(3) Any interception that does not comply with the terms of the court order shall be unlawful under section 3.

(4) Any authorization under a court order to intercept a communication shall be valid only for as long as it is necessary to achieve the purpose of the interception or, in any event, for a period not exceeding 90 days, after which, the said interception shall be deemed unlawful in accordance with section 3 unless its renewal is authorized under subsection (6).

(5) An application for renewal of a court order by the authorized officer shall be made ex parte and in writing to a judge of the High Court in Chambers and shall be accompanied by a sworn affidavit stating—
(*a*) the reason and period for which the renewal is required;
(*b*) details of the times, dates and the type of interception conducted under the court order, and of such information obtained from the said interceptions; and
(*c*) particulars of any previous applications involving the same person.

(6) The judge may renew a court order only once for a period not exceeding 90 days, after which time, any continued interception shall be deemed unlawful under section 3.

7. Termination of court order

(1) Where a court order has been terminated by the judge or has expired and has not been renewed, all intercepted material obtained under that court order shall be placed in a packet and sealed by the authorized officer, and that packet shall be kept away from public access.

(*d*) 將被截取通訊的形式及截取該通訊的方法；
(*e*) 獲授權人員可否任用根據《郵政署條例》(第 98 章) 或《電訊條例》(第 106 章) 授權的人協助他進行截取；
(*f*) 將被截取通訊的地方或有關設備的地點及性質的描述；
(*g*) 獲授權截取的期限；及
(*h*) 除第 9 條另有規定外，可向其披露被截取的材料的人士。

(2) 就第 (1)(*h*) 款而言，法官可授權向調查在第 (1)(*b*) 款所指罪行的其他執法人員披露被截取的材料。

(3) 任何不遵守法官在法令內的規定的截取，即在第 3 條下屬非法。

(4) 任何在法令下授權的截取只在有需要達至該截取的目的，或在任何情況，不超過 90 日之下，屬有效，否則除根據第 (6) 款獲授權續期外，在這以後的截取，即被視為在第 3 條下屬非法。

(5) 獲授權人員可單方面連誓章以書面向在內庭的高等法院法官申請法令的續期，誓章須列明——
(*a*) 要求續期的理由及期限；
(*b*) 在法令下進行的截取的詳細時間、日期及形式，及該截取所獲得的資料；及
(*c*) 在以前的申請中涉及相同的人士的詳情。

(6) 法官可批准一次不超過 90 日的續期，在這以後，繼續截取，即被視為在第 3 條下屬非法。

7. 法令的終止

(1) 凡被法官終止或已逾期仍未續期的法令，在該法令下獲得的被截取的材料須放在一包裹內，由獲授權人員封蓋，而該包裹須放在公眾取不到的地方。

(2) Where a charge is laid against the person named in the court order, the authorized officer shall notify the judge who may order the release of the intercepted material to the prosecutor where the latter intends to tender the intercepted material as evidence in criminal proceedings.

(3) Where the prosecutor intends to tender the intercepted material as evidence in criminal proceedings, he shall notify the accused of this intention at least 10 days before the trial date and furnish him with—

(*a*) a copy of the application made under section 5;

(*b*) a copy of the court order;

(*c*) a copy of the application for renewal of the court order, if any.

(4) Any information obtained by an interception that, but for the interception, would have been privileged remains privileged and inadmissible as evidence without the consent of the person enjoying the privilege.

(5) Where no charge is laid against the person named in the court order within 90 days of the termination of a court order, the court shall inform the authorized officer of its intention to—

(*a*) destroy the intercepted material in the sealed packet; and

(*b*) notify the person named in the order that his communications have been intercepted,

and shall give the authorized officer 5 days to inform the court whether or not he wishes to challenge the court's intentions.

(6) Where the authorized officer wishes to challenge the court's intentions stated in subsection (5)(*a*) or (*b*), he shall in writing provide the judge with his reasons for opposing the court's said intentions and it shall remain within the judge's discretion whether or not to accept these reasons.

(7) Where—

(*a*) the authorized officer does not inform the court of his intention to challenge the court's intentions stated in subsection (5)(*a*) or (*b*) within 5 days; or

(*b*) after considering the authorized officer's reasons for preventing the court from carrying out its intentions, the court decides not to accept his reasons,

the court shall order that all intercepted material in the sealed packet be destroyed immediately and shall notify the person named in the order that his communications have been intercepted, providing in the notice details on—

(i) the type of communication that was intercepted;

(ii) the time and date of each interception; and

(iii) the reasons for conducting the interception.

(8) Where the judge exercises his discretion not to order the destruction of intercepted material, he may make an order to specify the period for which the intercepted material will remain undestroyed.

(2) 凡在法令內被指明的人被控，獲授權人員須通知法官，以便控方欲在訴訟中提交被截取的材料作為證據時，該法官可發出命令把被截取的材料交予控方。

(3) 凡控方欲在訴訟過程中提交被截取的材料作為證據，他須在審訊日期前 10 日通知被告這意圖及提供予被告——

(*a*) 根據第 5 條提出的申請書的副本；

(*b*) 法令的副本；

(*c*) 如有，法令續期申請書的副本。

(4) 在假若沒有該截取的情況下，任何截取所獲得的資料，不用享有保密特權的人的同意，若該資料已受該特權涵蓋將繼續受涵蓋及不被接納為證據。

(5) 凡在法令終止後 90 日內，在法令內被指明的人未被控罪，法院須通知獲授權人員其意圖以——

(*a*) 銷毀放在封蓋包裹內的被截取的材料；及

(*b*) 通知在法令內被指明的人他曾被截取通訊，

及給予獲授權人員 5 日限期以通知法院他是否欲反對法院的該意圖。

(6) 凡獲授權人員欲反對法院在第 (5)(*a*) 或 (*b*) 款所述的意圖，他須向法官以書面提出其反對法院的該些意圖的理由，由法官酌情決定是否接納該些理由。

(7) 凡——

(*a*) 獲授權人員在 5 日內沒有通知法院其意圖反對法院在第 (5)(*a*) 或 (*b*) 款所述的意圖；或

(*b*) 法院在考慮獲授權人員阻止法院實行其意圖的理由，並決定不接納其理由，

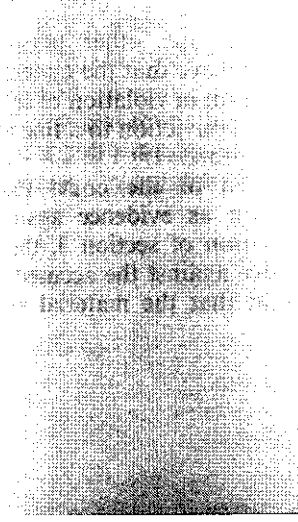
法院須命令立即銷毀所有放在封蓋的包裹內的被截取的材料，及通知在法令內被指明的人他曾被截取通訊，並在通告內提供以下詳情——

(i) 被截取通訊的形式；

(ii) 每次截取的日期及時間；

(iii) 進行截取的理由。

(8) 凡法官行使其酌情權在不下令銷毀被截取的材料，他可命被截取的材料在指定期限內不被銷毀。



PART V

SAFEGUARDS FOR INTERCEPTED MATERIAL

8. Safeguards

An authorized officer shall make arrangements to ensure that the following requirements are satisfied—

(*a*) that the following are limited to the minimum that is necessary having regard to the purposes specified in section 4(2)—

(i) the extent to which the intercepted material is disclosed;

(ii) the number of persons to whom any of the intercepted material is disclosed;

(iii) the extent to which the intercepted material is copied; and

(iv) the number of copies made of any of the intercepted material; and

(*b*) the intercepted material is destroyed as soon as its retention is not necessary for any of those purposes, including any criminal proceedings arising from any of those purposes or an order is made under section 7(7).

PART VI

DISCLOSURE AND ADMISSIBILITY OF EVIDENCE

9. Disclosure and admissibility of evidence

(1) A person who intentionally discloses to any other person any intercepted material knowing or having reason to believe that the material was obtained through the interception of a communication in violation of section 3 shall be guilty of an offence and liable on summary conviction to a fine at level 4 and to imprisonment for a term not exceeding 2 years.

(2) In any proceedings, if it is represented to the court that the intercepted material relied on by the prosecution as evidence against the accused was or may have been obtained in violation of section 3, the court shall not allow the material to be given as evidence against the accused unless the prosecution proves beyond reasonable doubt that the material was not obtained as aforesaid.

第 V 部

被截取的材料的保障

8. 保障

獲授權人員須安排以滿足下列規定——

(*a*) 在考慮第 4(2) 條指明的目的的情況下，在有需要時，限制以下的範圍至最低標準——

(i) 披露被截取的材料的範圍；

(ii) 接受披露任何被截取的材料的人數；

(iii) 複製被截取的材料的範圍；及

(iv) 複製任何被截取的材料的數目；及

(*b*) 為任何目的，包括由於任何目的而產生的任何訴訟過程中，或根據第 7(7) 條發出的法令，而沒有需要保留被截取的材料時，須盡快銷毀該被截取的材料。

第 VI 部

資料披露及接納證據

9. 資料披露及接納為證據

(1) 任何人意圖向其他任何人披露被截取的材料，而他是知道或有理由相信該材料是在違反第 3 條下截取所獲得，即屬犯罪，一經循簡易程序定罪，可處第 4 級罰款及監禁不超過 2 年。

(2) 在訴訟過程中，如法庭獲指示控方依據被截取的材料作為指控被告的證據，是在違反第 3 條下獲得的，除控方證明無合理疑點下，法院該信納該材料不是按前述所指所獲得的，否則法院須取消該材料作為證據。

(3) The court can of its own motion require the prosecution to prove that the intercepted material was not obtained in violation of section 3.

(4) A person who is authorized under section 4 to intercept a communication, oral or otherwise, shall not disclose the intercepted material to any other person or persons save those named in the court order under section 6(1)(*h*).

(5) A person who receives any intercepted material under section 6(1)(*h*) and intentionally discloses the material to any other person who is not named in section 6(1)(*h*) shall be guilty of an offence and liable to a fine at level 4 or to imprisonment for 2 years or both.

(6) A person who intercepts a communication in accordance with the Post Office Ordinance (Cap. 98) or the Telecommunication Ordinance (Cap. 106) who otherwise than in the course of duty, or in assisting an authorized officer under a court order, intentionally discloses to any person any of the intercepted material shall be guilty of an offence.

(7) Subsections (1), (4), (5) and (6) do not apply to a person who discloses the intercepted material for the purposes of giving evidence in any proceedings.

(8) In any proceedings, the court may refuse to admit intercepted material as evidence against the accused if it appears to the court that having regarded to all the circumstances, including the grounds upon which the interception was authorized and the application procedure for the authorization, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it.

PART VII

REMEDIES

10. Remedies

(1) This Part applies to an interception of a communication in the course of its transmission by post or by means of telecommunication system through the use of any electro-magnetic, acoustic, mechanical or other device in contravention of section 3.

(2) For the purposes of this Part, a person is an aggrieved person if and only if—

(*a*) the person was a party to the communication; or

(*b*) the communication was made on the person's behalf.

(3) 法院可自行要求控方證明被截取的材料不是在違反第 3 條下獲得的。

(4) 任何人根據第 4 條獲授權截取口頭或其他通訊，不可向其他任何人 (在第 6(1)(*h*) 條下所指的在法令內被指明的人除外) 披露被截取的材料。

(5) 任何人根據第 6(1)(*h*) 條收取任何被截取的材料，並故意向任何其他沒有在第 6(1)(*h*) 條下被指明的人披露該材料，即屬犯罪，可處第 4 級罰款或監禁 2 年或兩者。

(6) 任何人根據《郵政署條例》(第 98 章) 或《電訊條例》(第 106 章) 截取電訊，除在履行職務或協助在法令內獲授權人員之外，故意向任何人披露任何被截取的材料，即屬犯罪。

(7) 第 (1)、(4)、(5) 及 (6) 款不適用於任何人為在訴訟過程中提供證據而披露被截取的材料。

(8) 在任何訴訟過程中，法院在考慮所有情況，包括授權截取的理由及申請授權的程序，覺得接納證據會對訴訟過程的公平性有不利效果，以至法院不應接納為證據時，法院可拒絕接納被截取的材料為證據。

第 VII 部

補救事宜

10. 補救事宜

(1) 本部分適用於在違反第 3 條下截取郵遞通訊，或在使用任何電磁、傳音、機械或其他裝置透過電訊系統傳遞的通訊過程中截取通訊的情況。

(2) 就本部而言，如屬下述情況的任何人即屬受屈——

(*a*) 該人為該通訊的一方；或

(*b*) 該通訊是為該人代表的。

(3) If a person ("the defendant")—

(*a*) intercepted a communication in contravention of section 3; or

(*b*) disclosed intercepted material to another person in contravention of section 9(1) or (5),

a court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the interception or the disclosure of intercepted material by making such orders against the defendant as the court considers appropriate.

(4) If a court convicts a person ("the defendant") of—

(*a*) an offence under section 3; or

(*b*) an offence under section 9(1) or (5),

the court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the interception or the disclosure of the intercepted material by making such orders against the defendant as the court considers appropriate.

(5) Without limiting the orders that may be made under this section against a person ("the defendant"), a court may make an order of one or more of the following kinds—

(*a*) an order declaring the interception or the disclosure of intercepted material, as the case requires, to have been unlawful;

(*b*) an order that the defendant pay to the aggrieved person such damages, including punitive damages, as the court considers appropriate; or

(*c*) an order in the nature of an injunction.

(6) Without limiting the orders that may be made by a court under this section, an order may—

(*a*) include such provisions as the court considers necessary for the purposes of the order; and

(*b*) be made either unconditionally or subject to such terms and conditions as the court determines.

(7) A court may revoke or vary an order in the nature of an injunction made by the court under this section.

(8) An application under subsection (3) for the grant of remedial relief is to be made within 6 years from the date on which the aggrieved person discovered the interception, or the disclosure of the intercepted material, as the case may be.

(9) An application under subsection (4) for the grant of remedial relief is not subject to any limitation period, but must be made as soon as practicable after the conviction concerned.

(3) 如任何人 ("被告人")——

(*a*) 在違反第 3 條下截取通訊；或

(*b*) 在違反第 9(1) 或 (5) 條下向其他人披露被截取的材料，

法院在接受受屈人的申請下，如認為合適，可命令被告人就該截取或該披露被截取的材料，給予受屈人補償。

(4) 如法院根據下列情況將某人定罪 ("被告人")——

(*a*) 在第 3 條下的罪行；或

(*b*) 在第 9(1) 或 (5) 條下的罪行，

法院在接受受屈人的申請下，如認為合適，可命令被告人就該截取或該披露被截取的材料，給予受屈人補償。

(5) 在不限制根據這條向任何人 ("被告人") 發出的法令的原則下，法院可發出以下的一項或多項法令——

(*a*) 宣布該截取、或該披露被截取的材料 (視屬何情況而定) 為非法的法令；

(*b*) 如法院認為合適，要求被告人給予受屈人賠償，包括懲罰性的損害賠償的法令；或

(*c*) 具禁制令性質的法令。

(6) 在不限制根據這條由法院發出的法令的原則下，某法令——

(*a*) 可包括就該法令而言，法院認為需要的條文；及

(*b*) 可在無條件下發出或在法院規定的條款或條件下發出。

(7) 法院可撤銷或更改在這條下由法院發出的具禁制令性質的法令。

(8) 根據第 (3) 款申請補償批准的，要在受屈人發現該截取，或該披露被截取的材料的日期 (視屬何情況而定) 起 6 年內提出。

(9) 根據第 (4) 款申請補償批准的，不受任何期限限制，但須在定罪後的切實可行期限內盡快提出。

PART VIII

POWER TO OBTAIN INFORMATION

11. Power to obtain information

The Legislative Council may at any time require the Secretary for Security to provide, for any specified period, the following information, namely—

(*a*) the number of interceptions authorized and denied;
(*b*) the nature and location of the facilities from which and the place where the communications have been intercepted;
(*c*) the major offences for which interception has been used as an investigatory method;
(*d*) the types of interception methods used;
(*e*) the number of persons arrested and convicted as a result of interceptions;
(*f*) the average duration of each interception; and
(*g*) the number of renewals sought and denied.

Consequential Amendments

Post Office Ordinance

12. Warrant of Chief Secretary for opening and delaying postal packets

Section 13 of the Post Office Ordinance (Cap. 98) is repealed.

13. Disposal of postal packets opened under section 10 or 12

Section 14 is amended by repealing "section 10, 12 or 13" and substituting "section 10 or 12".

14. Extension of sections 12 and 14 to articles not transmissible by post

Section 15 is amended by repealing "sections 12, 13 and 14" and substituting "sections 12 and 14".

第 VIII 部

獲取資料的權力

11. 獲取資料的權力

立法局可於任何時間要求保安司在任何指定期限內提供以下資料——

(*a*) 獲授權及被拒絕的截取的數目；
(*b*) 被截取通訊的地方及有關設備的性質及地點；
(*c*) 使用截取作為調查方法的重要罪行；
(*d*) 截取方法的形式；
(*e*) 截取所導致被逮捕及定罪的人數；
(*f*) 每次截取的平均期限；及
(*g*) 要求續期及被拒續期的次數。

相應修訂

《郵政署條例》

12. 布政司批出開啟和延遲處理郵包的手令

《郵政署條例》(第 98 章) 第 13 條現予廢除。

13. 對根據第 10 或 12 條開啟的郵包的處置

第 14 條現予修訂，廢除"第 10 、 12 或 13 條"而代以"第 10 或 12 條"。

14. 第 12 及 14 條引伸適用於不可藉郵遞傳送的物品

第 15 條現予修訂，廢除"第 12 、 13 及 14 條"而代以"第 12 及 14 條"。

Post Office Regulations

15. Regulation amended

Regulation 10 of the Post Office Regulations (Cap. 98 sub. leg.) is amended by repealing ", 12, or 13" and substituting "or 12".

Telecommunication Ordinance

16. Penalty for contravention of order under section 33

Section 30 of the Telecommunication Ordinance (Cap. 106) is repealed.

17. Power of Governor to prohibit transmission of messages, etc.

Section 33 is repealed.

《郵政署規例》

15. 修訂規例

《郵政署規例》(第 98 章，附屬法例) 的第 10 條現予修訂，廢除 "、12 或 13" 而代以 "或 12"。

《電訊條例》

16. 違反根據第 33 條所作命令的罰則

《電訊條例》(第 106 章) 第 30 條現予廢除。

17. 總督禁止發送訊息等的權力

廢除第 33 條。

Appendix IV

A comparison of the warrant systems for interception of communications in the HKSAR, the UK, the US and Australia

	Types of warrants	Issuing authorities
HKSAR	• No special classification of warrants.	• Under the Telecommunication Ordinance, all interceptions are ordered by the head of government; and • Both IOCO and the White Bill propose that all interception orders are issued by High Court Judges.
UK	• Normal warrants specify a person or a single set of premises; and • Certificated warrants apply solely to external communications outside the UK.	• All warrants are issued by the Home Secretary.
US	• Title III court orders authorize interception of contents of communications for law enforcement purposes; • FISA court orders authorize interception of contents of communications of foreign powers and their agents within the US for national security purposes; and • Pen/Trap court orders are issued to intercept non-content information of communications.	• Title III and Pen/Trap orders are issued by Judges of US District Courts or US Court of Appeals; and • FISA orders are issued by the FISA Court.
Australia	• Law enforcement warrants are issued for law enforcement purposes; and • National security warrants are issued for national security purposes.	• National security warrants are issued by the Commonwealth Attorney-General or the Director-General of Security; and • Law enforcement warrants are issued by eligible Judges or nominated Administrative Appeals Tribunal members.

Appendix IV (cont'd)

	Application procedures	Major grounds on which warrants are issued
HKSAR	• Under the Telecommunication Ordinance, only the head of government can order, or authorize any public officer to order, interception; • IOCO proposes that applications must be made by senior law enforcement officers; and • The White Bill proposes that only public officers of not lower than directorate rank or equivalent authorized by the head of government can apply for warrants.	• Under the Telecommunication Ordinance, whenever the head of government considers that the public interest requires; • IOCO proposes that court orders are required for preventing or detecting serious crimes or in the interest of the security of the HKSAR; and • The White Bill proposes that a warrant can be issued only for the purpose of preventing, investigating or detecting serious crimes, or the security of the HKSAR.
UK	• Applications must be made by the heads of law enforcement or security agencies.	• Warrant applications must meet the "*necessity*" and "*proportionality*" tests.
US	• Title III and FISA applications must be authorized by high-level judicial officials. Pen/Trap applications can be made by any attorney for the federal government.	• Title III and FISA applications must meet the "*probable cause*" test, while Pen/Trap applications are not required to do so.
Australia	• Applications for law enforcement warrants must be made by eligible authorities. Applications for national security warrant can be made only by the Director-General of Security.	• Law enforcement warrants can be issued only for the investigation of specified offences. National security warrants can be issued when the interception subjects may engage in activities prejudicial to national security or the information to be obtained is important to the national security of Australia.

Appendix IV (cont'd)

	Duration and renewal of warrants	Disclosure and admissibility of evidence
HKSAR	• The Telecommunication Ordinance has no provisions about these topics; • IOCO proposes that new court orders are valid for up to 90 days, and they can be renewed once for a period of up to 90 days; and • The White Bill proposes that new warrants are valid for up to six months, and there is no upper limit on the number of renewals made.	• The Telecommunication Ordinance has no provisions about these topics; • IOCO proposes that lawfully intercepted materials are admissible as evidence in court; and • The White Bill proposes that intercepted materials are not admissible as evidence in court, unless they are used to prove an illegal interception.
UK	• New warrants are valid for up to three months; and • Warrants can be renewed successively. Each renewal on serious crime grounds is valid for up to three months. Each renewal on national security or national economic well-being grounds is valid for six months.	• Intercepted materials are not admissible as evidence in court, except in limited circumstances.
US	• New Title III orders, new FISA orders and new Pen/Trap orders are valid for up to 30 days, 90 days, and 60 days respectively; and • All the three types of orders can be renewed successively for the same duration as their original orders.	• Lawfully intercepted materials are admissible as evidence in court.
Australia	• New law enforcement warrants are valid for up to 90 days and new national security warrants up to six months; and • Each type of warrants can be renewed successively for the same duration as their original orders.	• Lawfully intercepted materials are admissible as evidence in specified proceedings or circumstances.

Appendix IV (cont'd)

	Monitoring by executive authorities	Monitoring by judiciary
HKSAR	• No statutory mechanism for monitoring by the executive authorities is provided by the Telecommunication Ordinance, IOCO or the White Bill.	• The White Bill proposes to set up a Supervisory Authority, who is a Justice of Appeal and appointed by the head of government.
UK	• No statutory mechanism for monitoring by the executive authorities is provided by RIPA.	• The use of interception powers by intercepting agencies is monitored by the Interception of Communications Commissioner who is appointed by the Prime Minister and is a serving or retired Judge.
US	• No statutory mechanism for monitoring by the executive authorities is provided by the three interception statutes.	• Under Title III, the Judge who issues or denies a court order must report to the Administrative Office of the US Courts (the Administrative Office). Prosecutors must also submit annual reports to the Administrative Office providing information on their applications for court orders during the previous year; • Under FISA, the Attorney General must submit annual reports to the Administrative Office providing brief information on the issue of FISA warrants; and • Under the Pen/Trap statute, if a Pen/Trap device is used with any wiretap devices, such use must be reported to the Administrative Office.
Australia	• The Ombudsman is required to inspect at least twice every year the records of warrants maintained by the Australian Federal Police and the Australian Crime Commission, and report to the Attorney-General on the results of the inspections.	• No statutory mechanism for monitoring by the judiciary is provided by the Interception Act.

Appendix IV (cont'd)

	Monitoring by legislature	Monitoring by public
HKSAR	• The Telecommunication Ordinance does not provide for any mechanism for monitoring by the legislature; • IOCO proposes that the Legislative Council can require the Secretary for Security to provide information on interceptions conducted by the Government; and • The White Bill proposes that the head of government tables annual reports concerning the issue of interception warrants in the Legislative Council.	• No statutory mechanism for monitoring by the public is provided by the Telecommunication Ordinance, IOCO or the White Bill.
UK	• The expenditure, administration and policies relating to interception of communications conducted by security agencies are monitored by a statutory parliamentary committee known as the Intelligence and Security Committee. The Committee reports annually to the Prime Minister who tables the report in Parliament; and • The Interception of Communications Commissioner must submit annual reports to the Prime Minister who then tables the reports in Parliament.	• Members of the public who are aggrieved by interception activities can lodge complaints with the Investigatory Powers Tribunal, which can hear and determine complaints, award compensation and quash warrants.
US	• The Administrative Office must submit annual reports to Congress providing information on the particulars of Title III warrants; • The Attorney General must submit annual FISA reports to Congress, and fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence concerning surveillance under FISA twice every year; and • The Attorney General must submit annual reports on the particulars of Pen/Trap warrants to Congress.	• No statutory mechanism for monitoring by the public is provided by Title III, FISA or the Pen/Trap statute.
Australia	• The Joint Statutory Committee on the Australian Crime Commission has duties to examine the annual reports of the Australian Crime Commission (ACC), which can apply for interception warrants for law enforcement purposes, and to report to the Australian Parliament on the performance by ACC; and • The Parliamentary Joint Committee on ASIO, ASIS and DSD monitors the interceptions conducted by intelligence and security agencies.	• No statutory mechanism for monitoring by the public is provided by the Interception Act.