

立法會 *Legislative Council*

LC Paper No. CB(2)2776/05-06

Ref : CB2/BC/2/05

Paper for the House Committee meeting on 21 July 2006

Report of the Bills Committee on Interception of Communications and Surveillance Bill

Purpose

This paper reports on the deliberations of the Bills Committee on Interception of Communications and Surveillance Bill.

Background

2. The existing statutory provisions on interception of communications are contained in the Post Office Ordinance (Cap. 98), the Telecommunications Ordinance (Cap. 106) and the Interception of Communications Ordinance (Cap.532) (IOCO). Section 13 of the Post Office Ordinance empowers the Chief Secretary for Administration to authorise the Postmaster General or any or all of the officers of the Post Office to open and delay specified postal packets or specified classes of packets. Section 33 of the Telecommunications Ordinance empowers the Chief Executive (CE), when he considers that the public interest so requires, or any public officer authorised by him to order that any message or any class of messages be intercepted or detained or disclosed to the Government. IOCO was passed in June 1997, but CE has not appointed a day for it to come into operation. The Law Enforcement (Covert Surveillance Procedures) Order (the Executive Order) made by CE on 30 July 2005 sought to set out the legal procedures in accordance with which covert surveillance may be carried out by or on behalf of officers of law enforcement agencies.

3. In the judgment of *Koo Sze Yiu and Leung Kwok Hung v Chief Executive of the Hong Kong Special Administrative Region* handed down on 9 February 2006, the Court of First Instance (CFI) held that insofar as it authorises or allows access to, or the disclosure of, the contents of telecommunication messages, section 33 of the Telecommunications Ordinance is inconsistent with Articles 30 and 39 of the Basic Law and with article 14 of the Hong Kong Bill of Rights. CFI also made an order that

section 33 of the Telecommunications Ordinance and the Executive Order are valid and of legal effect for a period of six months in view of the legal vacuum which would be caused by the judgment.

4. In the judgment of *Leung Kwok Hung and Koo Sze Yiu v Chief Executive of the Hong Kong Special Administrative Region* handed down on 12 July 2006, the Court of Final Appeal (CFA) made an order to set aside the temporary validity order of CFI and substituted suspension of the declarations of unconstitutionality so as to postpone their coming into operation, such postponement will be for six months from the date of the CFI judgment of 9 February 2006. CFA stated that “the Government can, during the period of suspension, function pursuant to what has been declared unconstitutional, doing so without acting contrary to any declaration in operation. But, despite such suspension, the Government is not shielded from legal liability for functioning pursuant to what has been declared unconstitutional”.

The Bill

5. The Bill seeks to regulate the conduct of interception of communications and the use of surveillance devices by prescribed authorisations, by oversight of the Commissioner on Interception of Communications and Surveillance (the Commissioner) to be established under the Bill, and by regular reviews within the law enforcement agencies concerned.

6. The Bill also proposes to repeal IOCO and the existing section 13 of the Post Office Ordinance and to amend section 33 of the Telecommunications Ordinance.

The Bills Committee

7. At the House Committee meeting on 10 March 2006, Members formed a Bills Committee to study the Bill. The membership list of the Bills Committee is in **Appendix I**.

8. Under the chairmanship of Hon Miriam LAU Kin-yee, the Bills Committee has held 46 meetings (i.e. 60 two-hour sessions) with the Administration. The Bills Committee has also met with 10 organisations and individuals, and received written submissions from the Privacy Commissioner for Personal Data (Privacy Commissioner). The names of these organisations and individuals are listed in **Appendix II**. In addition, the Bills Committee has received briefings by the Administration on interception of communications, surveillance devices and the Police’s intelligence management system.

Deliberations of the Bills Committee

Main subjects of deliberations

9. The deliberations of the Bills Committee are set out in this report under the following subjects –

<u>Subject</u>	<u>Paragraphs</u>
(a) long title of the Bill;	10 - 11
(b) definition of covert surveillance;	12 - 20
(c) two-tier system for covert surveillance;	21 - 27
(d) surveillance device;	28 - 32
(e) definition of postal interception;	33 - 34
(f) conditions for issue, renewal or continuance of prescribed authorisation;	35 - 57
(g) prohibition on interception and covert surveillance;	58 - 62
(h) panel judges and authorisation given;	63 - 90
(i) application for judge's authorisation;	91 - 96
(j) executive authorisation;	97 - 102
(k) duration of prescribed authorisation;	103 - 108
(l) emergency authorisation;	109 - 119
(m) oral application;	120 - 126
(n) matters authorised, required or provided for by prescribed authorisation;	127 - 135
(o) device retrieval warrant;	136 - 140
(p) legal professional privilege;	141 - 151
(q) code of practice;	152 - 156
(r) Commissioner on Interception of Communications and Surveillance;	157 - 194
(s) regular review;	195 - 198

(t)	discontinuance of interception or covert surveillance;	199 - 206
(u)	safeguards for protected products and record keeping;	207 - 214
(v)	non-admissibility of telecommunications interception product;	215 - 221
(w)	non-compliance with the provisions in the Bill or the code of practice;	222 - 226
(x)	notification of targets of interception of communications or surveillance;	227 - 235
(y)	regulation and amendment of Schedules;	236
(z)	transitional arrangements; and	237 - 241
(aa)	proposal for a sunset clause.	242 - 246

Long title of the Bill

10. The long title of the Bill states that the Bill is to regulate the conduct of interception of communications and the use of surveillance devices by or on behalf of public officers and to provide for related matters. Some members consider that the long title should state that the Bill seeks to protect the freedom and privacy of communications of Hong Kong residents as provided in Article 30 of the Basic Law.

11. The Administration has responded that the Bill is not the only legislation that may be relevant to Article 30 of the Basic Law, particularly that it only seeks to regulate the conduct of public officers. The Administration, therefore, considers that the long title as presently drafted is an accurate reflection of the purpose of the Bill, and does not consider it necessary to include a reference to Article 30.

Definition of covert surveillance

12. Under the Bill, covert surveillance –

“(a) means any systematic surveillance carried out with the use of any surveillance device for the purposes of a specific investigation or operation, if the surveillance –

- (i) is carried out in circumstances where any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy;
- (ii) is carried out in a manner calculated to ensure that the person is unaware that the surveillance is or may be taking place; and

(iii) is likely to result in the obtaining of any private information about the person; but

(b) does not include any such systematic surveillance to the extent that it constitutes interception under this Ordinance.”

13. Clause 2(2) of the Bill provides that a person is not regarded as being entitled to a reasonable expectation of privacy within the definition of covert surveillance in relation to any activity carried out by him in a public place.

14. Members have questioned why the term “systematic” is included in the definition. Some members have asked whether the scope of covert surveillance includes undercover operations by law enforcement agencies. These members are concerned that any surveillance which is not systematic or planned would not be covered by the Bill. They are also of the view that undercover operations without the use of surveillance devices can be highly intrusive and should be regulated.

15. Some other members have enquired about the definition and the test of “reasonable expectation of privacy”. These members are concerned that clause 2(2) seems to suggest that a person talking on a mobile phone on the street or with a friend in a restaurant may be subject to surveillance and audio recording by law enforcement officers covertly without any requirement for authorisation.

16. The Administration has explained that the inclusion of the term “systematic” is to exclude immediate response to operational circumstances or cursory checks that form part of a law enforcement officer’s routine operation, e.g. in the course of patrolling a public place. To address members’ concern, the Administration has agreed to delete the term “systematic” in the definition of covert surveillance, and to amend paragraph (b) of the definition to the effect that covert surveillance does not include any spontaneous reaction to unforeseen events or circumstances, and any such surveillance to the extent that it constitutes interception under the Bill as enacted. The Administration has also agreed to introduce a Committee Stage amendment (CSA) to clause 2(2) to clarify that it would not affect the entitlement of the person in relation to words spoken, written or read by him in a public place.

17. Regarding undercover operations without the use of surveillance devices, the Administration has explained that the Bill only covers covert surveillance operations using devices. It is usual among common law jurisdictions to confine their relevant legislation to operations using devices. Undercover operations in Australia and the United States (US) do not require statutory authorisation. Undercover operations in Hong Kong are governed by the relevant internal guidelines of the law enforcement agencies.

18. The Administration has further explained that if an activity being monitored is carried out in a place which is accessible to the public, the monitoring without using a

device should not give rise to privacy concern. Where an activity takes place in private premises, the law enforcement agencies would be liable for trespass under common law and for any unlawful act that they may carry out on the premises, if they enter premises without lawful authority.

19. Hon Margaret NG has proposed a CSA to the definition of intercepting act to the effect that an undercover agent of the law enforcement agencies will be subject to the Bill. Hon Margaret NG has also proposed CSAs to delete the reference to “reasonable expectation of privacy” in the definition of covert surveillance.

20. Hon James TO has proposed a CSA to the definition of covert surveillance to the effect that an undercover agent of, or any person on the instruction of or under the control of, the law enforcement agencies will be subject to the Bill.

Two-tier system for covert surveillance

21. The Bill proposes a two-tier system for covert surveillance. Type 2 surveillance means any covert surveillance which is carried out with the use of a surveillance device by a party participating in the relevant activity, or it is carried out with the use of an optical surveillance device or a tracking device and the use of the device does not involve –

(a) entry onto any premises without permission; or

(b) interference with the interior of any conveyance or object without permission.

For Type 2 surveillance, authorisation will be given by an officer not below a rank equivalent to that of Senior Superintendent of Police, to be designated by the head of the respective law enforcement agency (paragraph 97 below refers).

22. Under the Bill, Type 1 surveillance means any covert surveillance other than Type 2 surveillance. The authority for authorising Type 1 surveillance will be vested in a panel judge (paragraph 63 below refers).

23. The Administration has explained that whether a covert surveillance operation is Type 1, i.e. “more intrusive” or Type 2, i.e. “less intrusive”, depends mainly on whether the surveillance is carried out by a party participating in the relevant communications. In general, operations involving the use of devices are considered more intrusive. On the other hand, when the use of devices involves a party participating in the relevant communication, e.g. an undercover agent, the operation is considered less intrusive because that party’s presence is known to the other parties and that party may in any case relate the discussion to others afterwards.

24. Members have enquired whether an authorisation for Type 1 or Type 2 surveillance would be sought when more than one type of surveillance devices or operations are involved. Some members consider that optical surveillance targeting bathrooms or changing rooms, or tracking devices that may be taken inside private premises should be excluded from the coverage of Type 2 surveillance. Some members consider that any surveillance activity involving the use of surveillance device should be Type 1 surveillance requiring authorisation by panel judges.

25. The Administration has responded that the level of authorisation required for a particular operation would depend on the circumstances. If an operation involves both Type 1 and Type 2 surveillance, the authorisation of a panel judge would be sought. To put this beyond doubt, the Administration has agreed to add a new provision to spell out the policy intent expressly.

26. The Administration has also advised that if the use of the optical surveillance device involves entry into premises without permission or interference with the interior of any object without permission, the surveillance would be Type 1 surveillance. Use of optical device from outside premises should have much less impact on the privacy of individuals inside the premises, and individuals can and do take further measures when they expect even greater privacy, e.g. closing the window and door when using a bathroom or changing room. The Administration has agreed to address these concerns by stating in the code of practice that extra care should be taken in planning operations that involve sensitive premises or situations.

27. Hon Margaret NG has proposed CSAs to the effect that Type 1 surveillance means any covert surveillance which is carried out by the use of any surveillance or tracking device, or involves entry into any premises without permission, or interferes with the interior of any conveyance or object without permission. Type 2 surveillance means any covert surveillance other than Type 1 surveillance.

Surveillance device

28. Some members have suggested that surveillance devices involving the implantation or swallowing of surveillance devices into a human body should be excluded from the Bill. These members are also concerned about the adverse impact of surveillance devices on the health of the subject. Hon James TO has suggested that the safety of a surveillance device should be certified by the Department of Health or health authorities in other jurisdictions.

29. The Administration has responded that it is unlawful to implant a device without the consent of the person or without express statutory authority. An authorization under the Bill would not constitute sufficient authority for authorising such action. In any event, the law enforcement agencies do not use surveillance devices in such a way. The proposed exclusion is unnecessary. However, in view of some members' concern, the Administration has agreed to introduce a CSA to put beyond doubt that a prescribed

authorisation does not authorise any device to be implanted in, or administered to, a person without the consent of the person.

30. Regarding the use of surveillance devices which are harmful to health, the Administration has explained that it is not aware that surveillance devices using present-day technologies have harmful effects, and it is the Administration's policy not to use devices known to be harmful to health. It has been the practice of the law enforcement agencies when acquiring new surveillance devices to take care to ensure that the devices do not have harmful health effects on either the targets of surveillance or law enforcement officers. The Administration will, in the code of practice to be issued by the Secretary for Security under clause 59 of the Bill, remind law enforcement agencies to assess the possible impact of a surveillance device on health before the device is first used.

31. Members have asked whether an authorisation for surveillance would cover the use of surveillance devices outside the territory of Hong Kong and the use of such devices within Hong Kong on targets outside Hong Kong.

32. The Administration has explained that the jurisdiction of law enforcement agencies covers Hong Kong only, and the Bill does not extend the jurisdiction of law enforcement agencies. Should devices be carried outside Hong Kong, signals from the devices may be received by law enforcement agencies in Hong Kong, depending on the circumstances. In the same way that interception may be carried out in Hong Kong on calls to or from mobile phones roaming outside Hong Kong, signals from such devices may legitimately be received by the law enforcement agencies in Hong Kong.

Definition of postal interception

33. Under the Bill, "postal interception" means interception of any communication transmitted by a postal service. Members have asked whether postal interception covers opening a postal article for the purpose of forensic examination of the contents, obtaining the name and address of the sender, changing the contents of a postal packet without reading the contents, or putting foreign contents into postal packets.

34. The Administration has explained that in the context of the Bill, interception of postal communications is given a broad meaning, encompassing the inspection of communications as well as other articles in a postal packet. Obtaining the fingerprints or checking the identity or address of the sender covertly would therefore fall under the definition of postal interception. On the other hand, postal interception of itself should not include replacing the contents of the communications or adding foreign contents into postal packets. In view of some members' concern, the Secretary for Security has undertaken to state this in his speech during the resumption of the Second Reading debate on the Bill.

Conditions for issue, renewal or continuance of prescribed authorisation

Proposals in the Bill

35. Under clause 3 of the Bill, authorisation for interception of communications and covert surveillance should only be given for the purposes of preventing or detecting serious crime, or the protection of public security. In addition to the specific purposes, authorisation should only be given where the test of proportionality is met, taking into account the immediacy and gravity of the case and whether the purpose sought can reasonably be furthered by other less intrusive means.

Definition of public security

36. Some members have queried whether the term “public security” includes national security and whether it is confined to the security of Hong Kong. They are concerned that in the absence of a definition, public security may be used for political purposes, or for suppressing the right to freedom of expression or the right of peaceful assembly, and whether interception of communication or covert surveillance would be carried out for offences under Article 23 of the Basic Law. Article 23 provides that the Hong Kong Special Administrative Region (HKSAR) shall enact laws on its own to prohibit any act of treason, secession, sedition, subversion against the Central People’s Government, or theft of state secrets, to prohibit foreign political organisations or bodies from conducting political activities in the HKSAR, and to prohibit political organisations or bodies of the HKSAR from establishing ties with foreign political organisations or bodies. These members have pointed out that the term “security” is defined in similar legislation of Australia, Canada and New Zealand. They have asked the Administration to consider providing a definition for the term “public security”.

37. The Administration has responded that terms such as security or national security are not defined in the relevant legislation of the United Kingdom (UK) and US. In Australia, Canada and New Zealand, although the term “security” is defined, the definitions tend to be broad. In Hong Kong, the term “public security” is not defined in the Law Reform Commission (LRC) report on the regulation of the interception of communications published in 1996, IOCO enacted in June 1997 and the LRC report on the regulation of covert surveillance published in 2006. The Bill follows that approach.

38. The Administration has further explained that public security cannot be confined to matters that cause a direct threat to Hong Kong. As a responsible member in the international community, Hong Kong has an obligation to assist in monitoring threats to other jurisdictions, such as bombing in another city. If Hong Kong assists others in thwarting a security threat, they are more likely to assist Hong Kong in case of a threat directed at Hong Kong. The Administration has assured members that no interception of communications or covert surveillance would be carried out for offences under Article 23 of the Basic Law which have yet to be created. The Administration has also assured members that the public security ground would not be used for political

purposes, nor for suppressing the right to freedom of expression or the right of peaceful assembly, and that the Bill is unrelated to the offences under Article 23 of the Basic Law. The Secretary for Security has undertaken to state this assurance in his speech during the resumption of the Second Reading debate on the Bill.

39. Having considered the views of members, the Administration has agreed to introduce CSAs to define public security as the public security of Hong Kong, and to expressly provide that advocacy, protest or dissent (whether in furtherance of a political or social objective or otherwise), unless likely to be carried on by violent means, is not of itself regarded as a threat to public security. The Administration will also move CSAs to require law enforcement agencies to include in the application for issue of prescribed authorisation for interception or covert surveillance an assessment of the impact, both direct and indirect, of the threat on the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong.

40. Some members have expressed concern about the threshold of “likely” in the proposed CSAs referred to in the above paragraph. The Administration considers that it is an appropriate test. The Administration explains that it may not be possible to ascertain beforehand whether such advocacy, protest, etc. will be carried out by violent means before it is carried out. Hence, only an assessment as to the likelihood may be carried out.

41. Hon Margaret NG has proposed CSAs to define public security as “the public security of Hong Kong from terrorists acts which present a clear and imminent threat to life or by acts immediately endangering public safety”. In addition, for the purpose of the Bill, the exercise of any right enjoyed by any person under the Basic Law or under international treaties, conventions or instruments applying to the HKSAR or under common law shall not be regarded as a threat to public security.

42. Hon James TO has proposed a CSA to the effect that public security means the public security of Hong Kong, but does not include economic security. Mr TO has also proposed CSAs to the effect that association, assembly, strike, confrontation, advocacy, protest or dissent, unless intended to be carried on by violent means, is not of itself regarded as a threat to public security. In addition, any acts prescribed under Article 23 of the Basic Law, unless intended to be carried on by violent means, is not of itself regarded as a threat to public security.

Definition of serious crime

43. Under the Bill, “serious crime” means any offence punishable –

- (a) in relation to the issue or renewal, or the continuance, of a prescribed authorisation for interception, by a maximum penalty that is or includes a term of imprisonment of not less than seven years; or

- (b) in relation to the issue or renewal, or the continuance, of a prescribed authorisation for covert surveillance, by a maximum penalty that is or includes a term of imprisonment of not less than three years; or a fine of not less than \$1,000,000.

44. Some members have pointed out that the scope of serious crime under the Bill is too broad. In respect of interception of communications, offences punishable by over seven years' imprisonment will in effect include all indictable offences. For covert surveillance, offences punishable by three years' imprisonment will include all indictable offences and many summary offences. For instance, the offence of robbery carries a maximum penalty of imprisonment for life. The offences of theft, obtaining property by deception, and false accounting would attract 10 years' imprisonment. Offences associated with organisation of unauthorised assembly, and unlawful assembly under the Public Order Ordinance (Cap. 245) carries a maximum sentence of three years' imprisonment upon conviction on indictment or summarily. These members consider that the Bill should only cover the most serious offences. They also consider that some highly intrusive covert surveillance, such as the use of bugging device to pick up conversations, should require a higher threshold as in the case of interception of communications.

45. The Administration has responded that setting the threshold of the seriousness of offences by reference to the maximum penalty for the offence is similar to the approach adopted in the 1996 LRC report, the White Bill published in 1997 and IOCO. As interception is considered to be a highly intrusive investigative technique, a higher threshold is necessary. On the other hand, there is a wide spectrum of covert surveillance operations with varying degrees of intrusiveness. Since surveillance operations in general can be more specific in terms of location, timing and event, they are less intrusive. It would be reasonable to impose a lower threshold on the crimes over which such investigative technique could be deployed.

46. The Administration has further explained that the serious crime threshold is but an initial screen. The other tests set out in clause 3 of the Bill, most importantly proportionality which in turn relates to the gravity and immediacy of the serious crime to be prevented or detected, must also be met. The Administration considers that for the purpose of initial screening, making reference to the maximum penalty level is appropriate.

47. The Administration has also informed members that the threshold in Australia in respect of telecommunications interception is offences punishable by imprisonment for at least seven years, and in respect of surveillance, relevant offences include those punishable by imprisonment of three years or more, a few other specific offences, and offences prescribed by the regulations. In UK, the threshold in respect of interception and intrusive surveillance is –

- (a) offences for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to three years of imprisonment or more; or
- (b) crimes that involve the use of violence, resulting in substantial financial gain, or are conducted by a large number of persons in pursuit of a common purpose.

For less intrusive forms of covert surveillance, no threshold is specified.

48. Hon Margaret NG has proposed CSAs to the effect that serious crime means any offence punishable by a maximum penalty of imprisonment of not less than seven years.

49. Hon James TO has proposed CSAs to the effect that in relation to the issue or renewal, or the continuance, of a prescribed authorisation for covert surveillance, serious crime means any offence punishable by a maximum penalty of imprisonment of not less than seven years.

The test of reasonable suspicion

50. Some members consider that one of the conditions for the issue or renewal, or the continuance, of a prescribed authorisation is that there is reasonable suspicion that any person has been, is, or likely to be, involved in a specific serious crime or any activity which constitutes or would constitute a threat to public security. The Administration has agreed to introduce the relevant CSAs.

The test of necessity

51. In response to members' suggestion, the Administration has agreed to spell out explicitly in the Bill that in addition to the test of proportionality, the test of necessity should be met before an authorisation should be given. The relevant CSAs will be moved by the Administration.

Other matters to be considered

52. Some members have expressed concern that the proportionality test is too restrictive. They have suggested that the authorising authority should give sufficient consideration to the human rights implications of interception or covert surveillance operations, and that an express reference to the Basic Law, in particular Chapter III which concerns the fundamental rights and duties of the residents, should be included in the Bill.

53. In response to members' concern, the Administration will introduce a CSA to the effect that the authorising authority would also consider other matters that are relevant in the circumstances. The Administration explains that the proposed provision is a wide

one allowing the authorising authority to take into account all matters that are relevant in the case. It does not preclude the consideration of relevant provisions of the Basic Law as appropriate. The panel judges would be aware of the need to take into account the relevant provisions of the Basic Law in considering applications. The Administration will specify in the code of practice that law enforcement officers should take into account the Basic Law. The Administration considers that an express reference to the Basic Law in the Bill is not necessary.

54. Some members have suggested that a public interest test should be provided in the Bill when considering an application for authorisation for interception or covert surveillance which involves journalistic material.

55. The Administration has responded that the proportionality test covers the full range of fundamental rights and freedoms, and requires the relevant authority to pay sufficient regard to such rights and freedoms of the affected persons in examining whether the proposed operation would have a disproportionate effect. Accordingly, the panel judges will take into account the importance of press freedom. The Administration will include this as a reminder in the code of practice for the reference of the law enforcement agencies. The interception or covert surveillance sought to be carried out by a law enforcement agency is bound to be in the public interest if all the conditions in the clause are met. The Administration considers that it is unnecessary to specifically include a public interest test.

56. Hon Margaret NG has proposed CSAs to the effect that the right to freedom and privacy of communication protected by Article 30 of the Basic Law will be a relevant factor to be considered by the authorising authority. The rights and freedom protected in the Basic Law and the International Covenant on Civil and Political Rights will also be a relevant consideration. Hon James TO has proposed similar CSAs.

Other amendments proposed by members

57. Hon Margaret NG has proposed CSAs to stipulate that the conditions for issue, renewal or continuance of a prescribed authorisation are for the purpose of preventing or detecting a serious crime which the applicant reasonably believes is about to or has taken place as the case may be, or protecting public security against a threat which the applicant reasonably believes to be imminent. In addition, there should be credible evidence to show a reasonable suspicion that the subject of the interception or covert surveillance has been, is, or likely to be, involved in committing the serious crime, or undertaking the activity which constitutes or would constitute a threat to public security.

Prohibition on interception and covert surveillance

58. Clauses 4 and 5 of the Bill prohibit public officers from directly or through any other person carrying out any interception of communications or covert surveillance,

unless pursuant to a prescribed authorisation. Some members have pointed out that the Administration's stance is that CE is not a public officer. These members are concerned that CE might conduct interception operations without being regulated. They suggest that an express provision should be included to prohibit CE from conducting such operations.

59. The Administration has responded that the main purpose of the Bill is to provide the "legal procedures" by which public officers in the law enforcement agencies may conduct interception of communications and covert surveillance without breaching Article 30 of the Basic Law. In the case of CE, there is no intention that he should be able to obtain authorisations to conduct interception operations under the Bill, and therefore the legal procedures in the Bill do not extend to him. There is no need to expressly prohibit CE from conducting such operations, since Article 30 already prohibits interception and covert surveillance activities other than those carried out in accordance with legal procedures.

60. The Administration has pointed out that one of CE's constitutional functions under Article 48 of the Basic Law is to be responsible for the implementation of the Basic Law. Infringement upon the privacy of communications other than in accordance with the Bill or other legal procedures would be contrary to Article 30. CE would therefore be in breach of the Basic Law if he were to inspect communications other than in accordance with the Bill or other legal procedures. Such action may, in a serious case, constitute a serious breach of the law or dereliction of duty for the purposes of Article 73(9) of the Basic Law, and may lead to the Legislative Council (LegCo) passing a motion of impeachment against him. The mere fact that the prohibition in clauses 4 and 5 of the Bill does not extend to CE would not absolve him from his duty to observe and implement Article 30 of the Basic Law.

61. Hon Margaret NG has proposed CSAs to the effect that CE, members of the Executive Council and bureau heads insofar as they are not public servants will also be covered by the Bill.

62. Hon James TO has proposed CSAs to the effect that CE and bureau heads will also be covered by the Bill.

Panel judges and authorisation given

Proposals in the Bill

63. Under the Bill, the authority for authorising all interception of communications and Type 1 surveillance operations will be vested in one of the three to six CFI judges who have been appointed by CE as panel judges. According to the Administration, extended checking will be conducted on these CFI judges prior to their appointment as panel judges. An authorisation issued or renewed by a panel judge pursuant to an application by a law enforcement officer is proposed to be called "judicial

authorization”. The Bill also proposes that a panel judge would act judicially but would not be regarded as a court or a member of a court.

Appointment of a panel of judges

64. Some members oppose the proposal that the panel judges will be appointed by CE. These members consider that such appointing power should be vested with the Chief Justice. They are concerned that if judges are appointed to the panel by CE, their independence in carrying out their judicial duties as CFI judges or their eligibility as CFI judge may be affected. They have also expressed concern about the resource implications on the Judiciary, and have asked the Administration to provide past statistics on interception of communications and covert surveillance conducted by the law enforcement agencies.

65. The Administration has explained that prior to making the appointments, CE would ask the Chief Justice for recommendations. The term of appointment would be fixed at three years, and it is proposed that CE would only revoke an appointment on the recommendation of the Chief Justice and for good cause. Judges appointed to the panel will receive no advantages from that appointment. They will continue to be judges and whatever they do while on the panel will in no way affect their continued eligibility as judges. Their appointment by CE to the panel would give no positive or negative incentives that might affect their independence when carrying out their duties as panel judges. The Administration has informed the Bills Committee that it has previously consulted the Judiciary on the proposal for CE to be the appointing authority of the panel judges on the recommendation of the Chief Justice, and the Judiciary’s position is that the proposal is acceptable.

66. The Administration has pointed out that the power of CE under Article 48 of the Basic Law includes, *inter alia*, the power to appoint and remove judges of the courts at all levels. Article 88 of the Basic Law further provides that the judges of the courts of the HKSAR shall be appointed by CE on the recommendation of the Judicial Officers Recommendation Commission. That function reflects the role of CE under the Basic Law as head of the HKSAR. The proposal for CE to appoint panel judges is in line with that role. There are many other statutory offices to which judges may be appointed, and CE is almost invariably the appointing authority.

67. The Administration has informed members that designating selected judges to deal with different types of cases is not uncommon in Hong Kong or overseas. The proposed appointment arrangement has taken into account this consideration and would be comparable with the arrangement elsewhere for the appointment to be made by a senior member of the government. For instance, in Australia, a Minister declares eligible judges and nominates members of the Administrative Appeals Tribunal to approve interception of communications. In UK, the Prime Minister appoints the Surveillance Commissioner for approving intrusive surveillance operations.

68. Regarding the resource implications, the Administration has assured members that it will discuss with the Judiciary the necessary resources required for the implementation of the proposals in the Bill. The Administration has also informed members that for the three-month period between 20 February and 19 May 2006, there were 151 cases of interception of communications, all of which would require panel judge's authorisation under the new regime proposed in the Bill. For covert surveillance, there were 238 cases, 44 of which would require a panel judge's authorisation under the new regime.

69. Having regard to some members' suggestion that panel judges should be appointed by the Chief Justice, the Administration has informed the Bills Committee that it had relayed the suggestion to the Judiciary. The Judiciary has confirmed that its position, i.e. the Administration's proposal is acceptable, remains unchanged.

70. Regarding Hon Margaret NG's suggestion that panel judges should be appointed on a personal basis, the Administration has explained that paragraph 4 of Schedule 2 to the Bill provides that a panel judge shall not be regarded as a court in performing any of his functions under the Bill. However, insofar as only eligible judges may be appointed as panel judges, it may be misleading to provide that they are appointed entirely in their personal capacity. The Administration, therefore, does not consider it appropriate to adopt the suggestion.

71. Hon Margaret NG has proposed a CSA to stipulate that the panel judges will be appointed by the Chief Justice. Hon Margaret NG has also proposed a CSA to the effect that the panel judges shall not sit as ordinary judges during their appointment as panel judges.

Extended checking on panel judges

72. Some members oppose that extended checking, i.e. the highest level of integrity check, should be conducted on the panel judges prior to their appointment, as these judges should have already undergone integrity checking prior to their appointment as a judge. It might also give the public an impression of a lack of trust in these judges. These members have queried why such checking has to be conducted.

73. The Administration has explained that there are three levels of checking, i.e. appointment checking, normal checking and extended checking, with the last one being the most extensive. Extended checking is applicable to all people to be appointed to the most senior positions in the Government, e.g. Principal Officials and senior civil servants, and those who have access to very sensitive information. The Administration has also explained that extended checking has been conducted on law enforcement officers with wide access to the more sensitive information arising from covert operations, and similar checks will be conducted on the panel judges, the Commissioner on Interception of Communications and Surveillance, and their staff.

74. The Administration has pointed out that extended checking comprises interviews with the prospective appointees, his referees and supervisors as well as record checks. The checking is more thorough in order to help the appointment authority assess if there is any possible risk in appointing a candidate to a position involving much sensitive information. It does not involve any form of political vetting, and no investigation will be conducted on the political beliefs or affiliations of a prospective appointee.

75. The Judiciary Administration has advised the Bills Committee that the Judiciary has not objected to the Administration's proposed extended checking of the panel judges.

76. At the request of some members, the Secretary for Security has undertaken to state in his speech to be made during the resumption of the Second Reading debate on the Bill that the Chief Justice will be advised if the pre-appointment checking of the panel judges indicates a risk factor.

Affiliation with political parties

77. Some members have queried whether it would be appropriate for the panel judges to have affiliation with political parties. These members are concerned about the impartiality and independence of the panel judges, if they are allowed to have affiliation with political parties.

78. The Administration has responded that the policy of political affiliation of judges is under consideration by the Panel on Administration of Justice and Legal Services

Powers and functions of panel judges

79. Some members consider that the panel judges should function as a court and authorisation should be given in accordance with judicial procedures. The Bills Committee has queried whether the reference to "act judicially" in paragraph 4 of Schedule 2 to the Bill is necessary as a panel judge is not regarded as a court. The Bills Committee has also enquired about the meaning of the powers, protection and immunities of the panel judges.

80. The Administration has explained that a judge of CFI has statutory and common law powers. His statutory powers are those set out in the High Court Ordinance (Cap. 4) and the Rules of the High Court. The protection and privilege of the judges and proceedings of CFI are common law ones. CFI judges enjoy protection from all liability from all civil action for anything done or said by them in the course of performing their functions. That protection extends to analogous tribunals other than courts of law.

81. At the suggestion of members, the Administration has agreed to delete the reference to “act judicially”. The Administration will also introduce CSAs to move paragraph 4 of Schedule 2, which provides for the powers and functions of a panel judge, to the main body of the Bill.

82. Some members have expressed disagreement that the authorisation given by a panel judge should be called “judicial authorization”, as the panel judge is not exercising a court’s functions. The use of the term might give the public an impression that such authorisation is given by a court. These members have suggested that the term “judge’s authorization” be used. The Administration has agreed to the suggestion and will introduce the relevant CSA.

83. Some members, including Hon Albert HO, Hon Margaret NG and Hon Ronny TONG, remain of the view that the panel judges should function as a court and authorisation should be given in accordance with judicial procedures.

84. Hon James TO has proposed CSAs to the effect that the authority for authorising all interception of communications and Type 1 surveillance will be any judge of CFI, instead of a CFI judge who has been appointed as a panel judge.

Operational arrangements in giving authorisation

85. Members have enquired about the operational arrangements of the panel judges in their performance of authorisation functions.

86. The Administration has explained that in processing an application, the panel judge would apply the tests set out in clause 3 of the Bill and follow the procedures in handling a case. In a normal case, a law enforcement agency would have to submit a written application, supported by an affidavit setting out the justifications for the application. The panel judge would consider the application in private, and give careful consideration as to whether the materials are sufficient to satisfy the tests of proportionality and necessity. If necessary, the panel judge may seek further information and clarification from the law enforcement agency concerned. In response to members’ suggestion, the Administration has agreed to move CSAs to state that a panel judge may consider an application in such manner as he considers appropriate.

87. Paragraph 1(2) of Schedule 2 provides that, without prejudice to the requirement that a panel judge shall consider an application made to him in private, the application may, where the panel judge so directs, be considered at any place other than within the court precincts. Some members have suggested that it should be expressly provided that the panel judges would not consider applications in the premises of the law enforcement agencies.

88. The Administration has responded that the decision as to where applications are to be heard rests with the panel judge. However, the Administration does not envisage

that the panel judges would consider applications on the premises of the law enforcement agencies. The Administration has consulted the Judiciary, which has advised that the panel judges would not deal with any application at the premises of law enforcement agencies. In view of members' concern, the Administration has agreed to introduce a CSA to expressly provide that the panel judges should not consider applications on the premises of law enforcement agencies.

89. Some members consider that the panel judge should give his reasons for the authorisation issued. Hon Margaret NG has proposed CSAs to provide for a panel judge, when considering an application, to order a hearing to be held in private and any informant questioned, or to determine the application without a hearing, and that the panel judge shall give his determinations in writing together with his reasons. Ms NG has also proposed CSAs to move paragraphs 2 and 4 of Schedule 2, which respectively concerns further powers of the panel judges to administer oaths and take affidavits and functions of the panel judges, to the main body of the Bill.

90. Hon James TO has proposed a CSA to the effect that a judge of CFI, when considering an application for the issue or renewal of an authorisation, may invite the Privacy Commissioner to make submissions as a special advocate in camera.

Application for judge's authorisation

91. Under the Bill, an application to a panel judge by a law enforcement officer for the issue of an authorisation for interception or Type 1 surveillance shall be made in writing and supported by an affidavit.

92. Members have suggested that the officer giving the approval for making the application for a panel judge's authorisation and the officer conducting the review under clause 54 should not be the same person.

93. The Administration has explained that the role of an approving officer is to consider whether the applications for a panel judge's authorisation are appropriate. A reviewing officer under clause 54 is to keep under regular review compliance by officers of the law enforcement agencies with the relevant requirements under the Bill. There is no conflict between these two roles and the Administration does not consider that there is a need to expressly provide in the Bill that officers performing the two roles should not be the same person, although in practice, they will not be the same officer. The Administration will spell this out in the code of practice.

94. Some members have suggested that an express provision should be included to prohibit the law enforcement agencies from re-submitting an application on the basis of the same information, if such application has already been turned down by a panel judge.

95. The Administration has responded that it does not envisage that the law enforcement agencies will submit the same application for authorisation after it has been refused. However, after a previous application has been refused, they may make a fresh application for legitimate reasons, e.g. the circumstances may have changed or new information is available. Since the law enforcement agencies will have to provide information about their previous applications in making an application, the panel judge will take that into account. The Administration will make it clear in the code of practice that a refused application should not be re-submitted.

96. At the suggestion of members, the Administration has agreed to introduce CSAs to require the following additional information to be provided in the application –

- (a) information on previous application(s) made;
- (b) the post of the officer making the application;
- (c) an assessment of the likelihood of the contents of journalistic material being obtained; and
- (d) the identity of the directorate officer who have approved the making of the application for interception or Type 1 surveillance authorisations.

Executive authorisation

97. Clause 14 of the Bill provides for an officer of a department to apply to an authorising officer of the department for the issue of an executive authorisation for any Type 2 surveillance. The application is to be made in writing and supported by a written statement made by the applicant which is to comply with the requirements specified in Part 3 of Schedule 3 to the Bill. Under clause 7 of the Bill, the head of a department may designate any officer not below a rank equivalent to that of Senior Superintendent of Police to be an authorising officer. Applications for authorisation of Type 2 surveillance operations will only be made by officers of departments specified in Part 2 of Schedule 1 to the Bill, namely, the Customs and Excise Department, Hong Kong Police Force, Immigration Department and the Independent Commission Against Corruption (ICAC).

98. Members have suggested that the rank of the authorising officer should be raised to that of a Chief Superintendent of Police. Some members consider that stringent procedures should be put in place to guard against possible abuse. For instance, only officers of the unit who handle the case should make an application to the authorising officer. The authorising officer should not be directly involved in the case concerned, and the applicant should not be the authorising officer. In addition, officers of the same crime formation should not be the authorising authority. Members have also asked about the number of officers at directorate rank point 1 (D1) in the law enforcement agencies.

99. The Administration has informed members that the respective numbers of D1 officers or equivalent in the Police, Customs and Excise Department and Immigration Department are 48, 3 and 2. As regards ICAC, the lowest directorate rank in their hierarchy is D2-equivalent, i.e. Assistant Director, and there are four officers at that rank.

100. The Administration has explained that having regard to the circumstances of individual departments, the level of authorising officers in the case of the Police, Customs and Excise Department and Immigration Department will be raised to the rank equivalent to the Chief Superintendent of Police or above. However, in the case of ICAC, the level should remain at Principal Investigator or above, as the lowest directorate rank in its hierarchy is the rank of Assistant Director. The arrangement will be spelt out in the code of practice.

101. The Administration has also explained that the heads of crime formations are usually Chief Superintendents of Police. At the macro level, many officers in the department may be involved in an investigation, and the degree of involvement may increase should the case be of a particular serious nature. It is the policy intent that an authorising officer should not be directly involved in the investigation of the case concerned, and the policy intent will be set out in the code of practice.

102. Hon James TO has proposed CSAs to the effect that the authority for authorising Type 2 surveillance will be a judge of the District Court, and that a judge of the District Court, when considering an application for issue or renewal of an authorisation, may invite the Privacy Commissioner to make submissions as a special advocate in camera.

Duration of prescribed authorisation

103. It is proposed in the Bill that a prescribed authorisation granted, i.e. a judge's authorisation or an executive authorisation granted, should be for a duration of no longer than three months beginning with the time when it takes effect, and should be renewable for periods of not exceeding three months each.

104. Members have queried the justification for the three-month period. Some members have expressed concern that there is no limit to the number of renewals. They have suggested that in applications for renewals, the aggregate length of covert operations should be required for cases where a long period of interception or surveillance operation has taken place.

105. The Administration has responded that the three-month period is only the maximum period and the authorising authority may authorise an operation of a shorter duration. The period is comparable with the regimes of other jurisdictions in this area. For renewal applications, Part 4 of Schedule 3 to the Bill already requires an applicant to provide additional information, stating whether the renewal sought is the first

renewal and, if not, each occasion on which the authorisation has been renewed previously, the value of the information obtained so far, and the reason why it is necessary to apply for the renewal. In addition, the conditions for granting authorisation under clause 3 would require the authorising authority to taken into account the intrusiveness of the operation in approving the renewal.

106. Regarding the suggestion made by some members that a maximum number of renewal should be set, the Administration considers that the suggestion is not practicable. The Administration explains that serious and organised crimes may take a long time to plan, and hence long-term monitoring is required. On each renewal, the authorising authority will have to consider the value and relevance of the information likely to be obtained by carrying it out. Unless valuable information continues to be obtained, it will be increasingly difficult to justify the continuation of the operation. The Commissioner may review cases involving long-term monitoring to ensure that the powers are not abused. The Administration has also agreed that any renewal of the same authorisation for more than five times should be reported to the Commissioner, and the number of such cases will be included in the Commissioner's annual report (paragraph 179(f) below refers). The Administration believes that these checks and balances built into the regime in the Bill will ensure that operations will not be longer than justified.

107. Hon Margaret NG has proposed a CSA to require the authorising authority, in considering an application for renewal, to take into account the total duration of the interception or covert surveillance as the case may be. Hon Margaret NG has also proposed a CSA to limit the duration of a prescribed authorisation to two years.

108. Hon James TO has proposed CSAs to require a judge of CFI or a judge of the District Court, in considering an application for renewal, to take into account the total duration of the interception or covert surveillance as the case may be.

Emergency authorisation

109. Clause 20(1) of the Bill provides for an officer to apply to the head of the department for the issue of emergency authorisation for interception of communications or Type 1 surveillance, if he considers that –

- “(a) there is immediate need for the interception or Type 1 surveillance to be carried out by reason of an imminent risk of –
 - (i) death or serious bodily harm of any person;
 - (ii) substantial damage to property;
 - (iii) serious threat to public security; or

(iv) loss of vital evidence; and

- (b) having regard to all the circumstances of the case, it is not reasonably practicable to apply for the issue of a judge's authorisation for the interception or Type 1 surveillance."

110. Clause 23 of the Bill requires the head of the department concerned to cause an officer of the department to apply to a panel judge for confirmation of the emergency authorisation, as soon as reasonably practicable after, and in any event within 48 hours beginning with, the time when the emergency authorisation takes effect.

111. Members have enquired about the circumstances under which emergency authorisation is needed, given that oral applications to the panel judges could be made, and the panel judges are on call 24 hours. Some members have expressed concern that the provision in clause 20(1)(b) may give rise to possible dispute as to whether law enforcement officers should in all cases try to contact a panel judge to apply for an authorisation first even in emergency situations. Some other members, however, consider that it is necessary to retain the clause so that law enforcement officers would try their best to contact the panel judges before an application for emergency authorisation is made.

112. The Administration has explained that emergency applications apply only to cases which would otherwise require a judge's authorisation. This type of applications can only be made if it is not practicable to apply for a judge's authorisation, including oral applications to the panel judge. For instance, emergency situations when authorisation to conduct the operation is required as soon as possible, and there is an imminent risk of death or seriously bodily harm of any person, substantial damage to property, serious threat to public security, or loss of vital evidence. A law enforcement officer should first consider whether it is practicable to contact the panel judges to apply for a judge's authorisation, and only when this is not practicable, then an application for emergency authorisation would be made. An application in the form of an affidavit has to be made to a panel judge within 48 hours of the issue of the emergency authorisation. The panel judge may confirm the emergency authorisation if he is satisfied that the conditions in clause 3 have been met. He may refuse to confirm the emergency authorisation or confirm the authorisation with variations specified by him. The Administration envisages that the need for emergency authorisation should not be frequent.

113. The Administration has informed members that where an application for confirmation of emergency authorisation cannot be made within 48 hours, e.g. due to unforeseen events such as traffic accident involving the applicant concerned, the information obtained pursuant to the emergency authorisation would be destroyed immediately. A report will be submitted to the Commissioner on Interception of Communications and Surveillance with details of the case.

114. Some members are of the view that even though an application fails to be made within 48 hours, the law enforcement officer should still submit to a panel judge the emergency authorisation issued and explain why this cannot be done. The information obtained should be retained for the sole purpose of the investigation by the Commissioner.

115. The Administration has responded that the role of the panel judge in the confirmation procedure is to consider the relevant applications for confirmation. Where a department fails to apply for a confirmation within 48 hours, the question of confirming the emergency authorisation would no longer arise. The question will then become why the department has failed to comply with the requirement, which is more appropriate for the Commissioner to consider. Moreover, there are other provisions in the Bill that provide various channels for the Commissioner to take follow-up action as he thinks fit. The Administration, therefore, considers it more appropriate for the head of departments to report to the Commissioner, rather than to the panel judges, in such cases.

116. The Administration has further explained that the destruction arrangements for information obtained from emergency authorisations are to ensure that the information obtained pursuant to a prescribed authorisation should, in a case where the authorisation is not confirmed, be destroyed. The Administration does not consider it appropriate, having regard to the privacy of the subject of such operations, for the information to be preserved for the purpose of investigation by the Commissioner. In any event, the head of department is required to include in the report to the Commissioner details of the case which would facilitate his review.

117. At the suggestion of some members, the Administration has agreed to set out in the code of practice –

- (a) the procedures for an application for the issue of emergency authorisation;
- (b) that an emergency authorisation takes effect at the date and hours specified by the head of department concerned when issuing the emergency authorisation; and
- (c) that as far as possible, applications for emergency authorisation should not be used.

118. Hon Margaret NG has proposed CSAs to provide for an emergency application to be made orally, and the head of a department to give reasons for the emergency authorisation issued in writing. In the case where a department fails to make an application for confirmation to a panel judge in 48 hours, the head of the department concerned shall submit a report to the Commissioner with details of the case. Any information obtained pursuant to the emergency authorisation shall be preserved for the

review or examination of the Commissioner. The panel judges are empowered to make orders when they refuse to confirm the emergency authorisation.

119. Hon James TO has proposed CSAs to require the head of a department to give reasons for the emergency authorisation issued. When considering an application for confirmation of an emergency authorisation, a judge of CFI may invite the Privacy Commissioner to make submissions as a special advocate in camera. A CFI judge may also invite the Privacy Commissioner to assist him in arriving at a conclusion of not confirming an emergency authorisation. In addition, where a judge of CFI refuses to confirm the emergency authorisation, he may make an order for the destruction of any further information or intelligence or record derived from such information obtained pursuant to the emergency authorisation.

Oral application

120. Under the Bill, an application for the issue or renewal of a prescribed authorisation may be made orally, if it is not reasonably practicable for the application to be considered in accordance with the relevant written application procedure. Such an application is required to be followed by an application in writing to the relevant authorising authority for confirmation within 48 hours beginning with the time when the prescribed authorisation or renewal takes effect. If no application for confirmation of the prescribed authorisation or renewal is made within the period of 48 hours, the law enforcement agency concerned will immediately destroy any information obtained pursuant to the authorisation, and submit a report to the Commissioner on Interception of Communications and Surveillance with details of the case.

121. Members have queried the circumstances under which oral applications for prescribed authorisation or renewal need to be made.

122. The Administration has explained that oral applications are to cater for urgent cases where it is not possible to follow the written application procedure, e.g. by putting all the information in writing. Provisions for oral applications are common in other jurisdictions, e.g. Australia, Canada and UK. The Administration envisages that the need for oral application for renewal should be infrequent.

123. Members have suggested that arrangements should be made for audio recording by the panel judges or by the applicants of oral applications for a judge's authorisation, or for an executive authorisation.

124. The Administration has informed members that oral applications made to the panel judges would be audio-taped as far as practicable. In cases where recording is not practicable, the panel judges will make a written record. In the case of executive authorisation, the approving authority will make a written record of the application. In any event, the applicant will need to submit a written application within 48 hours, with the supporting affidavit/affirmation and documents setting out the facts presented to the

authorising authority at the time of the oral application, for application for confirmation.

125. In response to members' enquiry, the Administration has confirmed that it will set out in the code of practice that written records will be made on the additional information provided to the authorising officer in respect of an application for executive authorisation.

126. Some members are not convinced of the need for oral applications. Hon Margaret NG and Hon James TO have separately proposed CSAs to delete the provisions for oral applications.

Matters authorised, required or provided for by prescribed authorisation

127. Under clause 29(4), a prescribed authorisation, other than an executive authorisation, may contain terms that authorise the interference with any property, whether or not of any person who is the subject of interception or covert surveillance concerned. Members have queried whether the existing mechanism for compensation for damage caused to property during law enforcement operations is sufficient in respect of covert operations, and whether a special compensation mechanism should be put in place.

128. The Administration has explained that the covert nature of the operations covered by the Bill necessarily places a limit on the extent of interference with property. Any interference will only be sanctioned with the express authorisation by a panel judge under the clause. The Administration envisages that the interference in the vast majority of cases would not result in any damage at all. Should there be any damage, it would be minimal. As a matter of policy, the Administration will make good any damage caused, and will specify this in the code of practice.

129. The Administration has also explained that it may not be practicable to introduce a compensation mechanism in the Bill. To offer compensation to the owner of the property being interfered with would blow the cover of the operation and might jeopardise the operation. Having regard to members' concern, the Administration will set out in the code of practice that the law enforcement agencies would be required to report to the Commissioner all instances of interference of property in the course of carrying out authorised operations under the Bill, should there be any damage to the property concerned. They will have to report to the Commissioner the remedial action that they have taken to make good the damage and, if the damage cannot be made good, the reasons. The Commissioner may then review the adequacy of the measures taken by the law enforcement agencies in this regard and, if he deems it appropriate, make reports to CE under clause 48, or make recommendations to the law enforcement agencies under clause 50.

130. Clause 29(5) requires any person specified in a prescribed authorisation to provide to an officer of the law enforcement agency concerned assistance for the execution of the prescribed authorisation. Members have asked about the consequences for persons not providing the assistance under the clause, and whether it would amount to an offence of obstructing a police officer in the execution of his duty.

131. The Administration has confirmed that the failure of a person to provide assistance to law enforcement agencies under clause 29 would not attract criminal liability. In addition, such refusal would not amount to contravention of the various legislative provisions in respect of obstructing or failure to assist a public officer in the execution of his duty.

132. Under clause 29(7)(a)(ii), a prescribed authorisation may authorise the entry, by force if necessary, into premises, and into any other premises adjourning or providing access to the premises, in order to carry out any conduct authorised or required to be carried out under the prescribed authorisation.

133. Having regard to members' concern about the use of force, the Administration will introduce a CSA to clause 29(7)(a)(ii) to explicitly provide that reasonable force would be used if necessary. Similar amendment will be made to clause 29(7)(b)(ii) and (c)(ii).

134. Hon Margaret NG has proposed CSAs to require specifications, e.g. the identity of the person or persons whose communications are to be the subject of interception, in the prescribed authorisations issued.

135. Hon James TO has proposed various CSAs to clauses 29 and 30 of the Bill. One of the CSAs is to require that an assessment of risk and damage arising from the entry of any premises by use of force to be submitted to the authorising authority before the determination of the authorisation.

Device retrieval warrant

136. Clause 32 of the Bill provides that where a prescribed authorisation has ceased to have effect, an officer of the department concerned may apply to a panel judge for the issue of a device retrieval warrant authorising the retrieval of any of the devices authorised to be used under the prescribed authorisation. Under clause 34, a device retrieval warrant ceases to have effect upon the expiration of the period specified by the panel judge when issuing the warrant, which in any case is not to be longer than three months beginning with the time when it takes effect.

137. Members have expressed concern that an officer of the department concerned may not apply for a device retrieval warrant. Members consider that surveillance devices installed should be retrieved as soon as possible. Members have pointed out that when a prescribed authorisation has ceased to have effect, there is no legal basis for

the devices to remain in or on any premises. Members have suggested that provisions should be made to require an officer of the department to make an application to a panel judge, if the department concerned considers that it is not practicable to retrieve a device used.

138. The Administration has responded that it is its policy to try and retrieve surveillance devices after use as soon as reasonably practicable. This will be specified in the code of practice. The Administration has also explained that in some cases, it may not be practicable to retrieve a surveillance device after an operation. Retrieving the device might expose the covert operation or endanger the safety of the law enforcement officers concerned. It is also possible that the target has already discovered the device, and the need to retrieve the device does not arise then. It is intended that the law enforcement agencies should report to the Commissioner all instances where they have not applied for a device retrieval warrant for devices not yet retrieved after the expiry of an authorisation and the reasons for not doing so. The Commissioner may then review the information provided and the reasons given by the law enforcement officers and, if he deems it appropriate, make reports to CE under clause 48 or make recommendations to the law enforcement agencies under clause 50.

139. Hon Margaret NG has proposed a CSA to the effect that a panel judge shall give his reasons for the issuance of a device retrieval warrant.

140. Hon James TO has proposed CSAs to require a judge of CFI, when considering an application for a device retrieval warrant, to take into account the assessment of the risk and damage arising from the retrieval of surveillance device to the premise or object. A judge of CFI shall give reasons for the issuance of a device retrieval warrant. If the judge of CFI refuses to issue the device retrieval warrant, he shall make an order directing the relevant head of the department to disable the function of the device.

Legal professional privilege

141. Clause 2(3) of the Bill provides that any covert surveillance which is Type 2 surveillance is regarded as Type 1 surveillance if it is likely that any information which may be subject to legal professional privilege (LPP) will be obtained by carrying it out. This means that such surveillance operations will require authorisation by a panel judge.

142. Some members have expressed concern about the protection of LPP. These members have queried the circumstances under which interception of communications and covert surveillance operations would be conducted in respect of lawyers and the safeguards for LPP. They have pointed out that under Article 35 of the Basic Law, Hong Kong residents shall have the right to confidential legal advice. Without sufficient safeguards against abuse, there could be a temptation for law enforcement officers to listen to LPP communications even though they know that they cannot retain the communications or use them in court. If clients know or even suspect that the

communications they have with their lawyers could be intercepted by law enforcement agencies, it may deter them from seeking legal advice or from speaking frankly with their lawyers. They consider that sufficient statutory safeguards should be put in place to guard against any intentional or inadvertent access to and use of LPP materials by the law enforcement agencies. They have suggested that in the course of a duly authorised interception of communications or surveillance operations, if certain communications are found to be subject to LPP, the interception or surveillance should stop immediately. In addition, without the consent of the person entitled to waive the privilege, the LPP materials should remain inadmissible as evidence before the court.

143. The Administration has pointed out that under the common law, LPP applies to communications between a client and his legal adviser, whether oral or in writing, if those communications are for the purpose of obtaining legal advice, except when such communications are in furtherance of a criminal purpose. There can be no exceptions to this privilege, unless the client waives it or it is overridden by statute, either expressly or by necessary implication. In drafting the Bill, the Administration has given full regard to this common law principle at various stages of the covert operations. At the stage of approval of operations or collection of information, the Bill preserves LPP by not overriding it, thereby requiring the law enforcement agencies and the panel judges to observe it when formulating and considering applications respectively. The Bill further requires that the law enforcement agencies and the panel judges consciously take into account the likelihood of obtaining information which may be subject to LPP in the application for and consideration of authorisations. These provisions would ensure that no covert operations under the Bill would knowingly seek to obtain information subject to LPP.

144. The Administration has informed the Bills Committee that it does not envisage that a judge will approve an operation targeting the communications at a lawyer's office or residence, unless the judge agrees that there are reasonable grounds to believe that the communications in question would be used for the furtherance of a crime, or the lawyer himself is criminally involved in an alleged offence.

145. Nevertheless, to address members' concerns, the Administration has agreed to introduce CSAs to the Bill to expressly reflect its policy intent of prohibiting operations targeting the communications at a lawyer's office, or any other premises ordinarily used by him for the purpose of providing legal advice to clients, or residence, unless –

- (a) the lawyer, or any other person working in his office or residing in his residence, is a party to any activities that constitute or would constitute a serious crime or a threat to public security; or
- (b) the communications in question is for the furtherance of a criminal purpose.

146. Regarding the discontinuance of operations, the Administration has pointed out that under clause 55(2) (a) and (b) of the Bill, the officer concerned –

- (a) shall, as soon as reasonably practicable after he becomes aware that any ground for discontinuance of the prescribed authorisation exists, cause the interception or covert surveillance to be discontinued; and
- (b) may at any time cause the interception or covert surveillance to be discontinued.

As far as LPP materials are concerned, the provision in (a) above will require the officer to stop the operation when, in the circumstances of the particular case, the conditions for the continuance of the prescribed authorisation under clause 3 are no longer met by reason of, e.g. LPP information being more likely to be obtained and thus the operation becoming more intrusive. The provision in (b) above will enable the officer to stop an operation in other cases.

147. The Administration has also explained that during an authorised covert operation, operational arrangements will be put in place to minimise the extent of disclosure of any materials subject to LPP which are inadvertently obtained. Such operational arrangements for all interception and Type 1 covert surveillance operations include –

- (a) the actual monitoring is by dedicated units of the law enforcement agencies. These units are strictly separated from the investigators;
- (b) these units are under instruction to screen out information protected by LPP, and to withhold such information from the investigators. The latter will only be provided with information after any LPP information has already been screened out;
- (c) the exception to the above arrangement is in operations involving immediate threats to the safety or well-being of a person, including the victims of crimes under investigation, informants, or undercover officers in a participant monitoring situation or in situations that may call for the taking of immediate arrest action. In such cases, there may be a need for the investigators to listen to the conversations in real time. If this is necessary, it will be specified in the application to the panel judges, and the panel judges will take this into account in deciding whether to grant an authorisation and, if so, whether any conditions should be imposed. After such an operation, investigators monitoring the operations will be required to hand over the recording to the dedicated units, who will screen out any LPP information before passing it to the investigators for their retention; and

- (d) for operations that are likely to involve LPP information, the law enforcement agencies will be required to notify the Commissioner. In other cases, the law enforcement agencies will also be required to notify the Commissioner if information involving LPP is obtained inadvertently.

148. The Administration has informed the Bills Committee that on the basis of the notification, the Commissioner for Interception of Communications and Surveillance may, *inter alia*, review the information passed on by the dedicated units to the investigators to check whether it contains any information subject to LPP that should have been screen out. The arrangements in paragraph 147 above will be spelt out in the code of practice, the compliance of which will be subject to the oversight of the Commissioner.

149. As regards the use and destruction of LPP products, the Administration has pointed out that as information subject to LPP may be inadvertently collected, there are safeguards in governing the use and destruction of products or information in clause 56(1) of the Bill. Taking into account members' concerns, the Administration has agreed to introduce CSAs to the Bill to expressly provide that products obtained in the course of a duly authorised interception of communications or covert surveillance operation that is protected by LPP remains privileged and shall not be used in any way unless they are necessary for the prosecutor to carry out his duty to ensure a fair trial in a future proceeding in respect of postal interception and covert surveillance products. CSAs will also be made to expressly provide that –

- (a) in respect of products from interception of telecommunications operations, they should be destroyed as soon as possible and no copy of the products should be retained; and
- (b) in respect of products from postal interception and covert surveillance operations, they should be destroyed as soon as possible unless their retention is required for the purposes of legal proceedings.

150. As for the use of LPP materials as evidence, the Administration has agreed to introduce CSAs to expressly provide that any information subject to LPP that has been obtained during a covert operation will continue to be privileged. This means, among other things, that the information in question could not be given as evidence without the consent of the client concerned.

151. Hon Margaret NG has proposed CSAs to further restrict exceptional circumstances warranting interception or covert surveillance at a lawyer's office or residence.

Code of practice

152. Under clause 59 of the Bill, the Secretary for Security shall issue a code of practice for the purpose of providing guidance to the law enforcement officers in respect of matters provided in the Bill.

153. Hon James TO has suggested that the code of practice for ICAC should be issued by the Secretary for Justice, in order to avoid giving the public an impression that ICAC is under the purview of the Secretary for Security.

154. The Administration has responded that the code of practice is intended to provide practical guidance to the law enforcement officers. The Secretary for Security will issue the code pursuant to the power conferred on him under the Bill. The procedural steps apply across the board among the law enforcement agencies. It is appropriate for the Secretary for Security who is designated under the Bill to issue one code applicable to all.

155. At the request of members, the Administration has agreed that the code of practice will be published as a general notice in the Gazette. The Administration will also provide the Panel on Security with the updated versions of the code of practice from time to time.

156. Hon Emily LAU has suggested that the Commissioner should take into account the views of Members when making his comments or recommendations on the code of practice to the Secretary for Security. The Administration has agreed to refer the suggestion to the Commissioner. The Bills Committee has suggested that the matter should be followed up by the Panel on Security.

Commissioner on Interception of Communications and Surveillance

Proposals in the Bill

157. Under the Bill, the Commissioner is proposed to be appointed by CE on the recommendation of the Chief Justice for a term of three years. A Justice of Appeal of the Court of Appeal, a judge of CFI, and a former permanent judge of the Court of Final Appeal, a former Justice of Appeal of the Court of Appeal or a former judge of CFI would be eligible for appointment. The functions of the Commissioner are to oversee the compliance by law enforcement agencies and their officers with the relevant requirements, i.e. any provision of the Bill, the code of practice or any prescribed authorisation or device retrieval warrant concerned. Specifically, his functions would include conducting reviews on compliance by departments and their officers, carrying out examinations on an application made by a person who believes himself to be the subject of interception or covert surveillance, submitting reports to CE, and making recommendations to the Secretary for Security and heads of departments.

Appointment of the Commissioner

158. Some members consider that the Commissioner should be a retired judge, and have queried whether it is appropriate for a serving judge to work on a part-time basis as the Commissioner. Hon Margaret NG has suggested that the Commissioner should be appointed in his personal capacity.

159. The Administration has responded that to allow a wider pool of candidates, it is appropriate to include both serving and retired judges as eligible judges for appointment as the Commissioner. There are many instances of serving judges appointed to statutory positions. The Administration also understands from the Judiciary that the pool of retired judges resident in Hong Kong is very limited, and they may not be willing to take on the work. The Administration has consulted the Judiciary on the proposal that a serving judge appointed as the Commissioner should not be assigned to hear any cases during the term of his appointment as the Commissioner. The Judiciary has no objection to this proposal.

160. The Administration is of the view that it may be misleading to provide in the Bill that a judge is appointed as the Commissioner in his personal capacity.

161. Regarding some members' suggestion that a committee should be established as the independent oversight body, the Administration has pointed out that the proposal to appoint a single person as a statutory authority is a common practice in Hong Kong and overseas. For example, in Hong Kong, the Ombudsman and the Privacy Commissioner are the statutory authorities. In UK, the oversight authority for interception of communications under the Regulation of Investigatory Powers Act 2000 is the Interception of Communications Commissioner. In Australia, the Ombudsman performs the oversight function in respect of interception of communications for the investigation of crime. The proposal to appoint a Commissioner is also in line with the recommendation of the LRC report published in 1996.

162. In response to members' suggestion, the Administration has agreed to introduce a CSA to make it clear that the re-appointment of the Commissioner would be made by CE on the Chief Justice's recommendation.

163. Hon Margaret NG has proposed CSAs to restrict the eligibility for appointment of the Commissioner to retired judges of CFA, Court of Appeal and CFI. CE must give reasons for revocation of the appointment of the Commissioner, and such revocation shall be reviewable by a court of law.

164. Hon James TO has proposed CSAs to the effect that the appointment or revocation of the appointment of the Commissioner will be subject to the approval of LegCo.

Functions and powers of the Commissioner

165. Hon Margaret NG has proposed a CSA to state clearly that the Commissioner has the power to investigate complaints made by any person in relation to any interception or surveillance carried out with or without authorisation.

166. Hon James TO has proposed a CSA to the effect that the Commissioner will oversee the overall implementation of the Bill, except the functioning of judges of CFI and District Court in relation to the Bill. Mr TO has also proposed CSAs to provide the Commissioner with a general power to investigate any complaint of alleged cases of interception or covert surveillance.

167. In addition, Hon James TO has proposed a CSA to the effect that the Commissioner may require a head of the department to take such remedial action and make compensation as he considers reasonable and necessary.

Review of the work of the Commissioner

168. Some members have suggested that a committee should be established to review the work of the Commissioner.

169. The Administration has responded that the Commissioner would be provided with adequate support to facilitate the performance of his functions under the Bill. He would also be given wide powers under the Bill to demand information. His annual reports to CE would be tabled in LegCo. It is not necessary to create another committee to oversee the Commissioner's work. There is also no such arrangement in respect of other statutory authorities, e.g. the Ombudsman and the Privacy Commissioner.

Reviews by the Commissioner

170. At the suggestion of members, the Administration has agreed to introduce CSAs to explicitly provide that the Commissioner shall conduct reviews on the reports submitted to him on the failure of law enforcement agencies seeking a confirmation from a panel judge within 48 hours of an emergency authorisation or an oral application, or non-compliance with any relevant requirement under clauses 23(3)(b), 26(3)(b)(ii) and clause 52 respectively.

171. Hon Margaret NG has proposed CSAs to state clearly the power of the Commissioner to conduct reviews on reports made to him under clause 23(3)(b), clause 24(3)(v) and clause 52. Hon Margaret NG has also proposed CSAs to provide the Commissioner with the power to require departments to investigate any contravention of the Bill and false information to obtain prescribed authorisation.

Examination by the Commissioner

172. Some members consider that the Commissioner should give more information to the person who has made an application for an examination to be conducted by the Commissioner if the Commissioner has found in that person's favour.

173. Hon Margaret NG has proposed CSAs to provide for the Commissioner to conduct examination if he considers or suspects that there is any case in which interception or covert surveillance has been carried out in contravention of the Bill. Ms NG has also proposed to allow the Commissioner not to carry out an examination if such an application is received more than five years, instead of one year as proposed in the Bill, after the day on which the interception or surveillance is alleged to have taken place. In addition, Hon Margaret NG has proposed a CSA to require the Commissioner to give reasons for his determination of an examination.

174. Hon James TO has proposed CSAs to provide for the Commissioner to conduct examination if he considers or suspects that there is any case in which interception or covert surveillance has been carried out in contravention of the Bill. In addition, if, on examination, the Commissioner determines that the interception or covert surveillance alleged has been carried out without the authority of a prescribed authorisation, he shall notify the applicant –

- (a) stating that he has found the case in the applicant's favour and indicating whether the case is one of interception or covert surveillance;
- (b) stating the broad nature of the interception or covert surveillance; and
- (c) stating the time when the interception or covert surveillance commences and the time when the interception or covert surveillance ends.

175. Hon James TO has proposed a CSA to allow the Commissioner not to carry out an examination if such an application is received more than five years, instead of one year as proposed in the Bill, after the day on which the interception or surveillance is alleged to have taken place. Mr TO has also proposed CSAs to the effect that the Commissioner shall not give reasons for his determination, give details of any interception or covert surveillance or indicate whether or not the interception or covert surveillance alleged has taken place, if the giving of such information would be prejudicial to the prevention or detection of crime or the protection of public security.

Findings and recommendations of the Commissioner

176. Members consider that the Bill should provide explicitly that the Commissioner can report his findings to the panel judges.

177. The Administration agrees that in some cases, the findings, determinations and recommendations of the Commissioner in the course of carrying out his duties could have some reference value to the panel judges. The Administration will introduce CSAs to provide that the Commissioner may also refer his findings in the reviews, determinations and recommendations to the panel judges, apart from CE and the Secretary for Justice.

178. At the request of members, the Administration has agreed to expressly provide in the Bill that on being notified of the findings in the reviews, determinations and recommendations of the Commissioner, the head of the department shall submit to the Commissioner a report with details of any measures taken by the department, including any disciplinary action taken in respect of any officer. The relevant CSAs will be made by the Administration.

Annual report

179. Having regard to members' suggestions for more detailed information in the Commissioner's annual report to CE, the Administration has agreed to include the following information in the annual report in addition to that provided in the Bill –

- (a) a breakdown by the types of authorisation, i.e. judge's authorisation, executive authorisation and emergency authorisation, in respect of the authorisations issued and refused, as well as renewals given and refused;
- (b) the respective number of notices given by the Commissioner under clause 43(2), i.e. in favour of the applicant, and clause 43(3), i.e. not in favour of the applicant;
- (c) the number of notification cases under the proposed notification mechanism referred to in paragraph 229 below;
- (d) the number of oral applications made, authorisations issued and refused;
- (e) the number of cases involving information subject to LPP;
- (f) the number of cases that have been renewed for more than five times;
- (g) the number and broad nature of any disciplinary action which has been taken in respect of any officer of a department according to any report submitted to the Commissioner;
- (h) the number and broad nature of any cases of error identified in the reviews by the Commissioner; and
- (i) the broad nature of recommendations made by the Commissioner under clause 48.

The relevant CSAs will be made by the Administration.

180. Regarding the request of some members that the report should include a breakdown by crime and public security cases, the Administration does not consider it

appropriate to provide such a breakdown nor major categories of public security cases. The Administration has explained that it could not preclude the possibility that the provision of any further breakdown would inadvertently disclose the operational details and capabilities of law enforcement agencies to the benefit of criminals. Australia and UK also do not disclose such breakdown. In US, although there is a statutory requirement for the statistics to be published in respect of authorisations given by the judges of the Foreign Intelligence Surveillance Court, the statutory requirement in this aspect is not as comprehensive as those proposed to be included in the Commissioner's report. Furthermore, in the LRC report on the regulation of covert surveillance published in 2006, LRC has also not recommended the provision of breakdowns in respect of the grounds for the issue of warrants in the annual reports to be furnished by the supervisory authority to LegCo.

181. Hon Margaret NG has proposed CSAs to expand the contents of the annual report.

182. Hon James TO has proposed CSAs to provide that information in the annual report should also include the following –

- (a) the respective numbers of authorisations issued or renewed for the purpose of preventing and detecting serious crimes, and for the purpose of protecting public security;
- (b) the major categories of threats to public security in respect of which prescribed authorisations have been issued or renewed;
- (c) the respective total numbers of telephone lines, facsimile lines, email accounts intercepted, and the total number of Internet Protocol addresses under surveillance;
- (d) the number of cases in which content of journalistic material has been obtained; and
- (e) the respective number of cases of departments in which disciplinary action has been taken in respect of any officer according to any report submitted to the Commissioner.

Tabling of the Commissioner's report in the Legislative Council

183. Under clause 47(4), CE is required to cause a copy of the Commissioner's annual report to be laid on the table of LegCo. However, under clause 47(5), if CE considers that the publication of any matter in the report would be prejudicial to the prevention or detection of crime or the protection of public security, he may exclude such matter from the copy to be laid on the table of LegCo. Under clause 48, the

Commissioner may from time to time submit any further report to the CE on any matter relating to the performance of his functions as he thinks fit.

184. Members consider that LegCo should be informed of any disagreement between the Commissioner and CE on matters to be excluded from the copy of the Commissioner's annual report to be laid on the table of LegCo. The Administration has agreed and will introduce a CSA to this effect.

185. Some members are of the view that matters which have been excluded from the Commissioner's report to be laid on the table of LegCo should be reported to LegCo. Any report made by the Commissioner to CE under clause 48 should also be laid on the table of LegCo. In addition, there should be in place a mechanism for LegCo to monitor the overall compliance with the relevant requirements by the law enforcement agencies. These members have suggested that the Administration should refer to the Commissioner the suggestion that the Commissioner should consider giving briefings to the Panel on Security in camera on such matters which have been excluded from the Commissioner's report, and overall compliance by the law enforcement agencies.

186. The Administration has explained that access to confidential information is governed by the "need to know" principle. It is appropriate for the Commissioner to have the flexibility of making confidential reports to CE.

187. Hon Emily LAU has suggested that a research study should be conducted on the monitoring of the work of law enforcement agencies in covert operations by legislatures in overseas jurisdictions, including the provision of confidential information to the legislatures in this regard. The Bills Committee has agreed that the proposed research study should be followed up by the Panel on Security.

188. Hon James TO has proposed a CSA to require matters excluded from the Commissioner's report under clause 47(5) to be reported to LegCo under confidential cover. Hon James TO has also proposed CSAs to require CE to laid on the table of LegCo a copy of the report made by the Commissioner under clause 48, together with a statement on whether any matter has been excluded from the report without the agreement of the Commissioner. If CE considers that the publication of any matter in the report would be prejudicial to the prevention or detection of crime, or the protection of public security, he may, after consultation with the Commissioner, exclude such matter from the report. Any matter which has been excluded from the report shall be reported to LegCo under confidential cover.

189. In addition, Hon James TO has proposed CSAs to require the Commissioner to laid on the table of LegCo a copy of his report on recommendations to departments. If the Commissioner considers that the publication of any matter in the report would be prejudicial to the prevention or detection of crime or the protection of public security, he may exclude such matter from the copy of the report. The matter excluded shall be reported to LegCo under confidential cover.

Supporting staff

190. Members have enquired about the staffing of the office of the Commissioner. Members have also asked whether the Commissioner will be held responsible for the management of his staff.

191. The Administration has advised members that there will be a Secretary at D1 level and 16 other supporting staff. It is implicit in the Commissioner's functions under the Bill that he may administer any staff to assist him to perform his functions. The Administration will make it clear to the Commissioner on his appointment.

192. Regarding Hon James TO's suggestion that provision should be made for the Commissioner to employ a legal adviser to assist the Commissioner, the Administration has advised that it would be up to the Commissioner to decide whether or not such staff should be employed. Resources would be allocated for the Commissioner to engage other professionals, including legal adviser, to assist him as he considers appropriate.

Access to sealed packets kept by panel judges

193. Some members consider that the Bill should explicitly provide that the Commissioner may request the panel judges to allow him to open sealed packets of documents or records kept by the panel judges for the Commissioner's examination.

194. The Administration has pointed out that clause 57 of the Bill imposes a duty on the law enforcement agencies to keep a proper record in respect of specified matters, including matters relating to applications for the issue or renewal of prescribed authorisations or device retrieval warrants, and other matters provided for in the Bill. The purpose of this arrangement is, *inter alia*, to enable the Commissioner to obtain the necessary information in order to properly conduct his reviews on the law enforcement agencies' compliance with the Bill, and the requirements under the code of practice and any prescribed authorisation. The law enforcement agencies will have to keep other documents and records to facilitate the Commissioner's performance of his duties. The need for the Commissioner to access the sealed packets kept by the panel judges should be minimal. In the rare circumstances that the Commissioner finds it necessary to access the documents kept by the panel judges, the Commissioner may approach the panel judges. Having regard to members' view, the Administration will include an express provision that the Commissioner may request access to the documents held by a panel judge and that the panel judge may comply with that request.

Regular review

195. Clause 54(1) of the Bill requires the head of each department to make arrangements to keep under regular review compliance by officers of the department

with the relevant requirements. Under clause 54(2), arrangements will be made for officers at a rank higher than those held by the authorising officers of the department to keep under review the exercise and performance by the authorising officers of any function under the Bill.

196. Members have pointed out that an emergency authorisation may be issued by the head of the department, and queried whether the review under clause 54(2) cover reviews of the issue of emergency authorisations by the heads of departments. Members have also enquired how an internal review of the issue of emergency authorisation would work.

197. The Administration has responded that an application for confirmation of the emergency authorisation has to be made to a panel judge within 48 hours from the time the authorisation is issued. The head of the department would ensure that the provisions in relation to the issue of emergency authorisation are complied with. How a department would conduct a review will be set out in the code of practice. The Administration has also advised that emergency authorisations are issued by heads of departments. As such, the review mechanism under clause 54(2) does not apply to them because that mechanism is designed to review the performance of authorising officers designated under clause 7 of the Bill. However, the issue of an emergency authorisation involves many steps. Most of them have to be undertaken by a law enforcement officer. Such compliance is subject to the regular review under clause 54(1).

198. On the frequency of regular reviews, the Administration has informed members that its intention is to have a general review at least every three months.

Discontinuance of interception or covert surveillance

199. Under clause 55 of the Bill, where, before an authorisation made ceases to be in force, the officer in the course of conducting a regular review or the officer in charge of the operation is satisfied that the conditions for the continuance of the prescribed authorisation under clause 3 are not met, or the purpose for which the authorisation was granted has been achieved, he will be required to cease the operation as soon as practicable, and notify the relevant authorising authority of the discontinuation of the operation. The authorising authority will then revoke the authorisation.

200. The Administration has explained that the provisions are to cater for situations where there are changes in circumstances such that the conditions under clause 3 are no longer satisfied, the operation should cease.

201. Members consider that clause 55(1) should be amended to make it clear that the reviewing officer may discontinue an operation at any time, and not only in the course of or further to a review. The Administration has agreed. The Administration has also agreed to delete clause 55(6)(b) as it is not strictly necessary. It will introduce the relevant CSAs.

202. Members have suggested that where an application for prescribed authorisation should not have been made and operations mistakenly conducted should also be included in the Bill as the grounds for discontinuance of a prescribed authorisation. Members have also suggested that a provision should be added to the effect that any authorisation shall cease to be in effect if there are significant changes, including changes in the likelihood of LPP or target's right of silence being infringed.

203. The Administration has agreed to introduce CSAs to require an assessment of the effect of an arrest on the likelihood that any information which may be subject to LPP will be obtained by continuing the interception or covert surveillance. The assessment should be submitted to the relevant authorising authority as soon as reasonably practicable after the arrest. The authority shall revoke the authorisation if he is satisfied that the conditions for the continuance of the operation are no longer met.

204. The Administration has also agreed to set out in the code of practice the requirement that an officer must be designated to be in charge of a covert operation for the purpose of clause 55(2), and that he should be made aware of the relevant information and developments that may constitute grounds for discontinuance. In addition, examples of conditions for continuance not being met will be set out in the code of practice.

205. Hon Margaret NG has proposed CSAs to the effect that the following will constitute grounds for discontinuance –

- (a) the application for, issuance or renewal of any prescribed authorisation is in contravention of the Bill; and
- (b) the interception or acts of covert surveillance carried out is in excess of the prescribed authorisation.

Hon Margaret NG has also proposed CSAs to provide for automatic discontinuance upon the arrest of persons subjected to interception or covert surveillance.

206. Hon James TO has proposed CSAs to the effect that following will constitute grounds for discontinuance –

- (a) the application for, issuance or renewal of any prescribed authorisation is in contravention of the Bill;
- (b) the interception or acts of covert surveillance carried out is in excess of the prescribed authorisation; and
- (c) the specified conditions in clause 31 are not met.

Safeguards for protected products and record keeping

207. Some members have suggested that provisions should be made so that covert surveillance products or records should be retained one year after all legal proceedings have been completed. The Administration has agreed and will introduce the relevant CSAs to clauses 56 and 57.

208. Hon James TO has suggested that the respective total numbers of telephone lines, facsimile lines and email accounts which have been intercepted, and Internet Protocol addresses under surveillance by the law enforcement agencies should be kept, and that such information should be provided to the Commissioner. The Administration has informed the Bills Committee that the code of practice will require the law enforcement agencies to keep such records. The Administration has also agreed to refer to the Commissioner the suggestion that he may wish to refer to such information.

209. Members consider that sufficient safeguards should be put in place to prevent possible abuse of retention and use of intelligence derived from interception of communications and covert surveillance activities. Some members have suggested that a mechanism should be established for the keeping and destruction of intelligence derived from such activities, and applying to a panel judge for the keeping of such intelligence. In addition, the Commissioner should be empowered to oversee the keeping of intelligence derived from covert operations. Members have also enquired about the criteria for determining whether or not intelligence obtained from covert operations should be kept.

210. The Administration has responded that information derived from covert operations would fall within the definition of products as long as they are the originals, copies, extracts or summaries of the products. The disclosure, protection and destruction of products obtained from covert operations are provided for under clause 56 of the Bill. Should there be any analysis which cannot be traced back to the products, such information will be kept by the law enforcement agencies only if it is useful for the purpose of prevention and detection of crime or the protection of public security. Any information that constitutes personal data is subject to the Personal Data (Privacy) Ordinance (Cap. 486).

211. The Administration has also explained that in the case of the Police, its intelligence management system is tightly controlled. The database is centralised, and the input is done by a dedicated unit separate from the investigative teams. The unit comprise officers specially trained and disciplined for the task, working under the charge of a Superintendent of Police. The system only contains information which is relevant to the prevention or detection of crime and safeguarding security of Hong Kong. Access to the database is also strictly controlled. All entries and retrievals are recorded, establishing an audit trail for inspection.

212. In the view of the Administration, the suggestion of establishing a mechanism for the keeping and destruction of intelligence derived from covert operations, and requiring an application to a panel judge for keeping such intelligence is not practicable. The Administration is also not aware of any common law jurisdictions requiring a similar arrangement.

213. The Administration has informed members that a comprehensive review of the intelligence management system of the law enforcement agencies will be conducted in a separate exercise with a view to further strengthening the systems, particularly to enhance the transparency of the policy on the use of such information. At the suggestion of members, the Administration has agreed to report to the Panel on Security the outcome of the review.

214. Hon Margaret NG has proposed CSAs to the effect that any information or intelligence report or record generated from the protected product will be subject to the same restriction and protection as the protected product. Hon Margaret NG has also proposed CSAs to require the departments to retain records in respect of matters relating to the applications for the issue or renewal of prescribed authorisations or device retrieval warrants, and other matters provided for in the Bill for a period of at least 10 years, instead of one year as proposed in the Bill.

Non-admissibility of telecommunications interception product

215. Under clause 58 of the Bill, any telecommunications interception product shall not be admissible in evidence in any proceedings before any court and shall not be made available to any party. Any evidence or question which tends to suggest matters relating to any application for the issue or renewal of any relevant prescribed authorisations, and other related matters shall not be adduced or asked. However, disclosure may be made to the judge in specified cases in the interests of justice.

216. Some members consider that the defence in criminal proceedings should be allowed to have access to telecommunications interception product and use it as evidence for the defence. These members have pointed out that the right to a fair trial is a fundamental right guaranteed under the Basic Law. The denial of the defence from access to telecommunications intercepts might violate the Hong Kong Bill of Rights Ordinance (Cap. 383). The decision of disclosure should be left to the trial judge, and not the prosecution. They have also queried whether evidence or information known to the prosecution but not the defence would satisfy the principle of equality of arms. They have pointed out that clause 58(3), which prohibits the asking of any questions about a prescribed authorisation for interception, changes the current practice of permitting inquiry into all of the relevant matters as part of the criminal proceedings. In addition, clause 58(4) as presently drafted could seriously limit the prosecution's duty of disclosure under common law. They have also pointed out that under clause 58(6),

the judge will only order disclosure to himself if he is satisfied that it is essential in the interests of justice. These members consider this a very high threshold.

217. The Administration has responded that it is its established policy that telecommunications intercepts will not be admissible in evidence in court proceedings. The proposals in the Bill are in line with the analysis and recommendations in the 1996 and 2006 LRC reports, and follow the UK practice in this regard. The Administration has explained that admitting in evidence material obtained through an interception of communications would require its retention for this purpose. This would run counter to the proposal of destruction of intercept products as soon as practicable. The use of intercept material as evidence would pose the risk of revealing the interception capability of the law enforcement agencies. It would also adversely impact on privacy by entailing the public dissemination of personal information.

218. The Administration takes the view that since neither the prosecution nor the defence may adduce any evidence from telecommunication intercepts, there is equality between the two sides in this respect. In the event that exculpatory material is identified during the course of an investigation, the direction of the trial judge will be sought and the judge may order disclosure of information. If the judge considers that the inability to produce the intercept products would result in an unfair trial, he may stay the proceedings. There should be no question of unfairness to the defence.

219. Having regard to members' concerns, the Administration has agreed to move CSAs to require the disclosure of exculpatory information to the trial judges. Under the proposed CSAs, where, for the purposes of any criminal proceedings (including appeal proceedings), any information obtained pursuant to a relevant prescribed authorisation and continuing to be available to the department concerned and might reasonably be considered capable of undermining the case for the prosecution against the defence or of assisting the case for the defence, the department shall disclose such information to the prosecution. The prosecution shall then disclose the information to the trial judge in an *ex parte* hearing held in private. The trial judge may then make such orders as he thinks fit for the purpose of securing the fairness of the proceedings. Where any such order is made, the prosecution shall disclose to the judge for any related proceedings the terms of the order and the information concerned in an *ex parte* hearing held in private.

220. Hon Margaret NG has proposed CSAs to allow the use of intercepts by the defence.

221. Hon James TO is not convinced of the need for clause 58. He has proposed CSAs to delete the clause to preserve the present position on admissibility in evidence in court proceedings.

Non-compliance with the provisions in the Bill or the code of practice

222. Some members consider that penalty provisions should be added for non-compliance with the provisions of the Bill or the code of practice.

223. The Administration has responded that as the Bill regulates government entities, non-government parties will not be subject to the provisions in the Bill. It would create an anomaly if, for the same conduct, law enforcement officers but not others would be subject to a new criminal offence. The Administration will consider the need for introducing general criminal offences on unauthorised interception and covert surveillance at the next stage.

224. The Administration has further advised the Bills Committee that a breach under the Bill would be subject to disciplinary action, and this would be stipulated in the code of practice. An officer who deliberately conducts operations without due authorisation might also commit the common law offence of misconduct in a public office. Applicable laws will continue to apply to law enforcement officers, such as the provisions in the Crimes Ordinance (Cap. 200) imposing criminal sanctions against making false statements. The Commissioner may refer a case to the Secretary for Justice to enable the latter to consider whether there is sufficient evidence to bring a prosecution against the defaulting officer for criminal offence. In addition, any non-compliance would be subject to the scrutiny of the Commissioner, who may report such cases of irregularity to the heads of departments and to CE. Statistics of such cases would also be provided to CE in the Commissioner's annual report, which would be tabled in LegCo. In the view of the Administration, these measures are powerful to ensure that law enforcement agencies and their officers will comply with the law and the applicable procedures.

225. Hon Margaret NG has proposed a CSA to the effect that any contravention of the provisions of the Bill shall be a civil wrong actionable in equitable relief as well as damages.

226. Hon James TO has proposed CSAs to the effect that any contravention of the provisions for prohibition on interception under clause 4 or covert surveillance under clause 5 shall be an offence punishable with a maximum penalty of two years imprisonment. Non-compliance by any public officer or any other person to answer any question, or provide any information, document or other matter as directed by the Commissioner under clause 51 shall be an offence punishable with a maximum penalty of two years imprisonment.

Notification of targets of interception of communications or surveillance

227. Members have queried why a person whose communication sent to or by him had been intercepted by law enforcement agencies or he himself is the subject of covert surveillance operation will not be notified after such activities have discontinued. Members have also queried how the person could lodge complaint when he is not informed of such activities. Some members have suggested that a requirement to notify

targets of operations after such activities have discontinued should be put in place. Some other members, however, consider that only in cases of interception or covert surveillance mistakenly conducted, should the persons concerned be notified.

228. The Administration has advised the Bills Committee that the proposal of not notifying the targets of operations is in line with the recommendations of the LRC reports published in 1996 and 2006 as well as the practice in UK and Australia. Canada and US have a notification requirement which is limited to crime cases. It covers only authorised interceptions or interceptions applied for, and provides for exceptions to the requirement, e.g. to meet the needs of operations. The Administration has explained that there will be difficulties to impose a general notification requirement for the following reasons –

- (a) not all covert operations will result in arrests. The absence of any arrest resulting from such operations does not necessarily mean that the target is not involved in any threat to law and order or public security. It is possible that while an operation has not led to the arrest of the target, he in fact continues to pose threats to the community for some time after the operation. Notifying the target in such cases would likely serve to tip-off such person and his associates, making subsequent investigation with similar means more difficult;
- (b) in case the target is arrested and the investigation turns overt, disclosure of any details of such covert operations will still reveal information on the capability and modus operandi of law enforcement agencies to the criminal and those in the same criminal syndicates, if any. This would not only reduce the chance of successfully conducting similar covert operations on the same criminals again, but enable criminals, especially those criminal syndicates which are becoming increasingly organised and sophisticated, to evade justice;
- (c) even if the target turns out not being involved in a threat, informing him could raise suspicions among the real targets or otherwise prejudice an operation. If the wrong target were to be notified of the mistaken operation, he may knowingly or unknowingly alert the real suspect;
- (d) in order to protect the confidentiality of covert operations, the level of details that may be disclosed is limited. The benefit of notification would be small and outweigh the disquiet caused; and
- (e) a general notification requirement might require keeping all the relevant details in case notification might be needed. This would not be in keeping with the principle of destroying these details as soon as possible in order to protect privacy.

The Administration therefore considers that a general notification requirement is not appropriate.

229. Nevertheless, having considered members' suggestion of a mechanism for notifying the subject in cases where the operation was wrongfully conducted, the Administration has proposed to put in place a mechanism for notification in limited circumstances. Under the CSAs proposed by the Administration, if in the course of performing any of his functions under the Bill, the Commissioner considers that there is any case in which any interception or covert surveillance has been carried out by a department without the authority of a prescribed authorisation issued or renewed, the Commissioner shall give notice to the person concerned. The person concerned may apply for an examination in respect of the interception or covert surveillance within six months after receipt of the notice or within such further period as the Commissioner may allow. The other provisions which apply to examination cases will also apply, i.e. the use of the judicial review principles in examination, the arrangement for possible compensation, that the Commissioner shall not give such notice nor award compensation for so long as he considers that this would be prejudicial to the prevention or detection of crime or the protection of public security. The Commissioner is also not required to give any notice to a person if –

- (a) the person concerned cannot, after the use of reasonable efforts, be identified or traced;
- (b) the Commissioner considers that the intrusiveness of the covert operation on the person is negligible; or
- (c) in the case of interception, it is within the description of clause 4(2)(b), i.e. interception of telecommunications transmitted by radiocommunications, and clause 4(2)(c), i.e. any interception authorised, permitted or required to be carried out by or under any enactment other than the Bill.

230. The Administration has explained that in considering whether an operation has been carried out without the authority of a prescribed authorisation, the Commissioner is not confined to establishing the fact of whether a relevant authorisation has been issued. In case an authorisation is issued, he will also review the process by which the decision was reached to ensure that the application has been made in accordance with the prescribed procedures, as well as the implementation of the prescribed authorisation to ensure that the authorisation has been implemented in accordance with its terms. The Commissioner may therefore decide that there is a case to notify the subject –

- (a) if there has been an operation for which the department should have applied for an authorisation but has not in fact done so; and
- (b) if there has been an authorisation but in the view of the Commissioner, for example, a higher level of authorisation should have been applied for,

information that was available and that was likely to have affected the determination as to whether to issue the authorisation was not provided to the authorising authority, or the operation does not comply with the terms contained in the authorisation.

231. Regarding compensation, the Administration has advised that under clause 43(2)(b), the Commissioner may order the payment of compensation at the same time as notifying the subject without the need for him to make a claim himself. The Administration proposes to revise the arrangement for both examination and notification cases, so that the subject is asked whether he wishes the Commissioner to consider compensation, and if so, he may submit representations to the Commissioner. The Commissioner shall take the representations into account when considering the merit of the case in terms of payment of compensation under clause 43(2)(b) and (4). The relevant CSAs will be introduced by the Administration.

232. Some members are of the view that the wording of the CSAs “carried out without the authority of a prescribed authorization” proposed by the Administration may not be able to cover some cases of interception or covert surveillance mistakenly or wrongfully conducted. They also consider that the Commissioner should give reasons for his findings in giving notice to the person concerned.

233. The Administration has explained that the test “carried out without the authority of a prescribed authorization” is appropriate. The Administration has also pointed out that giving the duration and whether the case concerns interception or covert surveillance already strikes the right balance between providing the subject with some details and not jeopardising the covert nature of the operations.

234. Hon Margaret NG has proposed CSAs to provide for –

- (a) notifications to persons in cases of interception or covert surveillance which have been wrongly carried out or carried out without the authority of a prescribed authorisation;
- (b) reasons to be given for the Commissioner’s findings; and
- (c) compensation to be ordered by the Commissioner.

235. Hon James TO has proposed CSAs to provide for –

- (a) notifications to persons in cases of interception or covert surveillance which have been mistakenly or wrongfully carried out, or carried out in contravention of the Bill; and

- (b) the Commissioner to give information on the broad nature of the interception or covert surveillance, and the time when the interception or covert surveillance commences and the time when it ends.

Regulation and amendment of Schedules

236. At the request of members, the Administration has agreed to introduce CSAs to the effect that the regulation to be made by CE under clause 62 and any amendments to Schedules 1, 2, 3 and 4 published in the Gazette by CE in Council under clause 63 will be subject to the approval by LegCo (i.e. the positive vetting procedure).

Transitional arrangements

237. Under clause 65 of the Bill, any materials obtained by way of interception pursuant to an order issued or renewed under section 33 of the Telecommunications Ordinance before the Commencement of the Bill, as enacted, are also subject to clauses 56 and 58 as if they were product obtained pursuant to a prescribed authorisation.

238. The Administration has explained that the policy intent of the clause is to apply the proposed safeguards under the new regime on safeguards for materials and admissibility to the products that have been obtained before the Bill takes effect, so that such products will be subject to the same requirements, e.g. retention and destruction as with the newly obtained products under the new regime. Since the same privacy and policy considerations apply, the Administration considers it appropriate to apply the safeguards to pre-existing materials so as to better protect the privacy of the parties concerned.

239. In the light of the judgment of CFA referred to in paragraph 4 above, the Administration will introduce CSAs to clause 65 to make it clear that the provisions in the clause should not be construed as validating or authorising any telecommunications interception carried out pursuant to an order made under section 33 of the Telecommunications Ordinance before the commencement of the proposed Ordinance. In addition, the Administration will introduce CSAs to delete the reference to clause 58 in clause 65 to the effect that clause 58 will not apply to any telecommunications interception carried out pursuant to such an order nor to the materials obtained by carrying out such an interception.

240. Hon Margaret NG has proposed a CSA to preclude the construction of the Bill as authorising interception or surveillance which has been held unlawful by any court before the commencement of the Bill, if enacted.

241. Hon James TO has proposed CSAs to delete the reference to clause 58.

Proposal for a sunset clause

242. Some members consider that it is imperative to provide in the Bill a mechanism for review or repeal of the Bill as enacted in consultation with the public, given that the freedom and privacy of communication is a constitutional right and is fundamental to personal freedom and political freedom. In addition, there has been no public consultation on the Bill. These members have suggested that a sunset clause should be included in the Bill to the effect that the Administration will review the legislation, otherwise it will cease to have effect.

243. Some other members, however, do not consider that there is a need for a sunset clause. Hon LAU Kong-wah has suggested that the Administration should report to the Panel on Security the implementation of the Bill, if enacted, on a regularly basis, e.g. every six months. The Administration should also undertake to conduct a comprehensive review of the legislation two to three years after it has come into operation.

244. The Administration does not consider that there is a need to provide for a sunset clause in the Bill, given prior public discussions on relevant issues in the past 10 years, the consultations it has done prior to its formulation of the legislative proposal behind the Bill, and the Bill Committee's detailed and comprehensive deliberations on the Bill. As a result of such deliberations, the Administration has made a number of CSAs in response to members' views and suggestions.

245. The Administration is of the view that to the extent that the legislation is not time-limited, a sunset clause is not appropriate. It is also relevant that in some of the overseas examples noted by the Bills Committee, unlike the Bill, the relevant legislation has been enacted in less than a month. The Administration will keep the implementation of the new legislation under review.

246. Hon Margaret NG has proposed a CSA to provide for a sunset clause.

Committee Stage amendments

247. Apart from the CSAs discussed in the above paragraphs, the Administration has agreed to move other amendments to the Bill for the purpose of clarity or refinement. A full set of the draft CSAs to be moved by the Administration is in **Appendix III**.

248. Apart from the CSAs discussed in the above paragraphs, Hon Margaret NG has proposed other amendments to the Bill. A marked-up copy of the Bill showing the draft CSAs proposed by Hon Margaret NG is in **Appendix IV**.

249. Apart from the CSAs discussed in the above paragraphs, Hon James TO has proposed other amendments to the Bill. A marked-up copy of the Bill showing the draft CSAs proposed by Hon James TO is in **Appendix V**.

Resumption of the Second Reading debate on the Bill

250. The Bills Committee has raised no objection to the resumption of the Second Reading debate on the Bill at the Council meeting on 2 August 2006.

Follow-up actions by the Administration

251. The Administration has agreed –

- (a) to provide the Panel on Security with an updated version of the code of practice from time to time (paragraph 155 above refers);
- (b) to refer to the Commissioner the suggestion that he should take into account the views of LegCo Members when making his comments or recommendations on the code of practice to the Secretary for Security (paragraph 156 above refers);
- (c) to refer to the Commissioner the suggestion that he may wish to refer to the respective total numbers of telephone lines, facsimile lines and email accounts which have been intercepted, and Internet Protocol addresses under surveillance by law enforcement agencies (paragraph 208 above refers); and
- (d) to report to the Panel on Security the outcome of the review of the intelligence management system of law enforcement agencies (paragraph 213 above refers).

Follow-up action by the Panel on Security

252. The Bills Committee has suggested that the following matters should be followed up by the Panel on Security –

- (a) the proposed research study on monitoring the work of law enforcement agencies in covert operations by legislatures in overseas jurisdictions, including the provision of confidential information to the legislatures in this regard (paragraph 187 above refers); and

- (b) the suggestion that the Commissioner should take into account the views of Members in making his comments or recommendations on the code of practice to the Secretary for Security (paragraph 156 above refers).

Advice Sought

253. Members are invited to note the deliberations of the Bills Committee and the date for the resumption of the Second Reading debate on the Bill.

Council Business Division 2
Legislative Council Secretariat
20 July 2006

**Bills Committee on
Interception of Communications and Surveillance Bill**

Membership list

Chairman	Hon Miriam LAU Kin-yee, GBS, JP
Deputy Chairman	Hon LAU Kong-wah, JP
Members	Hon Albert HO Chun-yan Hon LEE Cheuk-yan Hon Martin LEE Chu-ming, SC, JP Dr Hon LI Kwok-po, GBS, JP Dr Hon LUI Ming-wah, SBS, JP Hon Margaret NG Hon Mrs Selina CHOW LIANG Shuk-yee, GBS, JP Hon James TO Kun-sun Hon Bernard CHAN, GBS, JP Hon CHAN Kam-lam, SBS, JP Hon Mrs Sophie LEUNG LAU Yau-fun, SBS, JP Hon SIN Chung-kai, JP Dr Hon Philip WONG Yu-hong, GBS Hon Jasper TSANG Yok-sing, GBS, JP Hon Howard YOUNG, SBS, JP Hon Emily LAU Wai-hing, JP Hon Timothy FOK Tsun-ting, GBS, JP Hon Tommy CHEUNG Yu-yan, JP Hon Audrey EU Yuet-mee, SC, JP Hon Vincent FANG Kang, JP Hon LI Kwok-ying, MH, JP Dr Hon Joseph LEE Kok-long, JP Hon Daniel LAM Wai-keung, SBS, JP Hon Jeffrey LAM Kin-fung, SBS, JP Hon Andrew LEUNG Kwan-yuen, SBS, JP Hon Alan LEONG Kah-kit, SC Hon LEUNG Kwok-hung Hon CHEUNG Hok-ming, SBS, JP Hon WONG Ting-kwong, BBS

Hon Ronny TONG Ka-wah, SC
Hon CHIM Pui-chung (up to 19 June 2006)
Hon Patrick LAU Sau-shing, SBS, JP

Total: 34 Members

Clerk Mrs Sharon TONG LEE Yin-ping

Legal Adviser Mr LEE Yu-sung

Date 20 June 2006

**Bills Committee on
Interception of Communications and Surveillance Bill**

Organisations/individuals who have given oral representation to the Bills Committee

1. Democratic Alliance for Betterment and Progress of Hong Kong
2. Youth Action 21
3. Hong Kong Bar Association
4. The Law Society of Hong Kong
5. Society for Community Organization
6. Hong Kong Human Rights Monitor
7. Mr TSANG Kin-shing
8. Mr LAM Chi-wai
9. Mr CHAN Chi-hing
10. Mrs Amy Y K LIU

INTERCEPTION OF COMMUNICATIONS AND
SURVEILLANCE BILL

COMMITTEE STAGE

Amendments to be moved by the Secretary for Security

<u>Clause</u>	<u>Amendment Proposed</u>
2(1)	<p>(a) In the definition of “copy” –</p> <p>(i) in paragraph (a)(i), by deleting “which identifies itself as such copy, extract or summary of such contents”;</p> <p>(ii) in paragraph (a)(ii), by deleting “record of” and substituting “record showing, directly or indirectly,”;</p> <p>(iii) in paragraph (b)(i), by deleting “which identifies itself as such copy, extract or summary of the material”;</p> <p>(iv) in paragraph (b)(ii), by deleting “which identifies itself as such transcript or record made of the material”.</p> <p>(b) In the definition of “court”, by deleting “section 53 and section 4 of Schedule 2” and substituting “sections 6(3A) and 53”.</p> <p>(c) In the definition of “covert surveillance” –</p> <p>(i) in paragraph (a), by deleting “systematic”;</p> <p>(ii) by deleting paragraph (b) and substituting –</p> <p>“(b) does not include –</p> <p>(i) any spontaneous reaction to unforeseen events or circumstances;</p>

and

- (ii) any such surveillance that constitutes interception under this Ordinance;”.

- (d) In the definition of “data surveillance device”, in paragraph (a), by adding “by electronic means” before “; but”.
- (e) In the definition of “head”, in the English text, by deleting “deputy of the” and substituting “deputy”.
- (f) In the definition of “interception” –
 - (i) in paragraph (a), by deleting “the communication” and substituting “that communication”;
 - (ii) in paragraph (b), by deleting “communications;” and substituting “any communication;”.
- (g) By deleting the definition of “judicial authorization” and substituting –

““judge’s authorization” (法官授權) means a judge’s authorization issued or renewed under Division 2 of Part 3 (and, where the context requires, includes a judge’s authorization to be issued or renewed under that Division);”.
- (h) In the definition of “maintain”, in paragraph (a), by deleting “relocate” and substituting “reposition”.
- (i) In the definition of “postal service”, by deleting everything after “means” and substituting “postal service to which the Post Office Ordinance (Cap. 98) applies;”.
- (j) In the definition of “public place”, in paragraph (b), by deleting “to the extent that they” and substituting “that”.
- (k) By deleting the definition of “transmitted”.

- (l) In the definition of “Type 2 surveillance” –
 - (i) by deleting “subsection (3), means any covert surveillance to the extent” and substituting “subsections (3) and (3A), means any covert surveillance”;
 - (ii) by deleting paragraph (a) and substituting –
 - “(a) is carried out with the use of a listening device or an optical surveillance device by any person for the purpose of listening to, monitoring or recording words spoken or activity carried out by any other person, if the person using the device –
 - (i) is a person by whom the other person intends, or should reasonably expect, the words or activity to be heard or seen; or
 - (ii) listens to, monitors or records the words or activity with the consent, express or implied, of a person described in subparagraph (i); or”;
 - (iii) in paragraph (b), by deleting “it”;
 - (iv) in paragraph (b), by deleting “and” and substituting “, if”;
 - (v) in paragraph (b)(ii), by adding “, or electronic interference with the device,” after “object”.
- (m) In the definitions of “行政授權”, “緊急授權”, “審查” and “器材取出手令”, in the Chinese text, by deleting “有此要求” and substituting “所需”.
- (n) In the definition of “監聽器材”, in the Chinese text, by

deleting paragraph (a) and substituting –

“(a) 指用以作出以下行為的任何器材：竊聽、監聽、監測或記錄任何談話或在談話中向任何人或由任何人所說的說話；但”.

(o) In the definition of “藉郵政服務傳送的通訊”, in the Chinese text, by deleting “郵件” and substituting “郵遞品”.

(p) By adding –

““journalistic material” (新聞材料) has the meaning

assigned to it by section 82 of the Interpretation and General Clauses Ordinance (Cap. 1);

“postal article” (郵遞品) has the meaning assigned to it by section 2(1) of the Post Office Ordinance (Cap. 98);

“public security” (公共安全) means the public security of Hong Kong;”.

2(2) By adding “, but nothing in this subsection affects any such entitlement of the person in relation to words spoken, written or read by him in a public place” before the full stop.

2 By adding –

“(3A) An officer of a department may apply for the issue or renewal of a prescribed authorization for any Type 2 surveillance as if the Type 2 surveillance were Type 1 surveillance, and the provisions of this Ordinance relating to the application and the prescribed authorization apply to the Type 2 surveillance as if it were Type 1 surveillance.”.

2

By adding –

“(5A) For the purposes of this Ordinance, advocacy, protest or dissent (whether in furtherance of a political or social objective or otherwise), unless likely to be carried on by violent means, is not of itself regarded as a threat to public security.”.

2(6)

- (a) In paragraph (a), by deleting “also regarded as being made orally if it is” and substituting “regarded as being made orally if it is made orally in person or”.
- (b) In paragraph (a), in the Chinese text, by deleting “亦”.
- (c) In paragraph (b), by deleting “also regarded as being provided orally if it is” and substituting “regarded as being provided orally if it is provided orally in person or”.
- (d) In paragraph (b), in the Chinese text, by deleting “亦”.
- (e) In paragraph (c), by deleting “also regarded as being delivered orally if it is” and substituting “regarded as being delivered orally if it is delivered orally in person or”.
- (f) In paragraph (c), in the Chinese text, by deleting “亦”.

2

By deleting subclause (7).

3(1)

- (a) In paragraph (a)(ii), by deleting “and”.
- (b) By adding –
 - “(aa) there is reasonable suspicion that any person has been, is, or is likely to be, involved in –
 - (i) where the purpose sought to be furthered

by carrying out the interception or covert surveillance is that specified in paragraph (a)(i), the particular serious crime to be prevented or detected; or

- (ii) where the purpose sought to be furthered by carrying out the interception or covert surveillance is that specified in paragraph (a)(ii), any activity which constitutes or would constitute the particular threat to public security; and”.

- (c) In paragraph (b), by deleting “proportionate to” and substituting “necessary for, and proportionate to,”.
- (d) In paragraph (b)(i), by deleting “, in operational terms,”.
- (e) In paragraph (b)(i), by deleting “and”.
- (f) In paragraph (b)(ii), by deleting the full stop and substituting “; and”.
- (g) In paragraph (b), by adding –
 “(iii) considering such other matters that are relevant in the circumstances.”.

3(2) In paragraph (a)(i), by adding “particular” before “serious”.

4(1) By deleting “through any other person” and substituting “indirectly (whether through any other person or otherwise)”.

5(1) By deleting “through any other person” and substituting “indirectly (whether through any other person or otherwise)”.

6(2) By deleting “, and may from time to time be reappointed”.

6 By adding –

“(3A) In performing any of his functions under this Ordinance, a panel judge –

- (a) is not regarded as a court or a member of a court; but
- (b) has the same powers, protection and immunities as a judge of the Court of First Instance has in relation to proceedings in that Court.”.

6

By adding –

“(4A) A person previously appointed as a panel judge may from time to time be further appointed as such in accordance with the provisions of this Ordinance that apply to the appointment of a panel judge.”.

11(2)

In paragraph (b)(ii), by deleting “a copy of any affidavit” and substituting “copies of all affidavits”.

12(2)

By deleting “its grant” and substituting “the renewal”.

17(2)

In paragraph (b)(ii), by deleting “a copy of any statement” and substituting “copies of all statements”.

18(2)

By deleting “its grant” and substituting “the renewal”.

20(1)

- (a) In the Chinese text, by deleting “權 —” and substituting “權：該人員認為 —”.
- (b) In paragraph (a), in the Chinese text, by deleting “該人員認為”.
- (c) In paragraph (b), in the Chinese text, by deleting “該人

員”。

- (d) In paragraph (b), in the Chinese text, by deleting “後，認為” and substituting “下，”。
- 23(3)
- (a) In the English text, by deleting “If no application for confirmation of the emergency authorization is made” and substituting “In default of any application being made for confirmation of the emergency authorization”。
 - (b) In paragraph (a), by deleting everything after “concerned” and substituting “; and”。
- 24(3)
- (a) In paragraph (b), by deleting “any information obtained by carrying out the interception or Type 1 surveillance concerned, to the extent”。
 - (b) In paragraph (b)(i), by deleting everything after the comma and substituting “any information obtained by carrying out the interception or Type 1 surveillance concerned; or”。
 - (c) In paragraph (b)(ii), by adding “any information obtained by carrying out the interception or Type 1 surveillance concerned” after the comma。
- 26(3)
- (a) In the English text, by deleting “If no application for confirmation of the prescribed authorization or renewal is made” and substituting “In default of any application being made for confirmation of the prescribed authorization or renewal”。
 - (b) In paragraph (b)(i), by deleting everything after “concerned” and substituting “; and”。

26

By adding –

“(4A) If, at the time of an application for confirmation of the prescribed authorization or renewal as provided for in subsection (1), the relevant authority is no longer holding his office or performing the relevant functions of his office –

- (a) without prejudice to section 54 of the Interpretation and General Clauses Ordinance (Cap. 1), the reference to relevant authority in that subsection includes the person for the time being appointed as a panel judge or authorizing officer (as the case may be) and lawfully performing the relevant functions of the office of that relevant authority; and
- (b) the provisions of this section and section 27 are to apply accordingly.”.

27(3)

- (a) In paragraph (b), by deleting “any information obtained by carrying out the interception or covert surveillance concerned, to the extent”.
- (b) In paragraph (b)(i), by deleting everything after the comma and substituting “any information obtained by carrying out the interception or covert surveillance concerned; or”.
- (c) In paragraph (b)(ii), by adding “any information obtained by carrying out the interception or covert surveillance concerned” after the comma.

- 29(6)
- (a) In paragraph (b), by adding “the use of reasonable” before “force”.
 - (b) By deleting paragraph (c) and substituting –
 - “(c) the incidental interception of any communication which necessarily arises from the interception of communications authorized to be carried out under the prescribed authorization; and”.
- 29(7)
- (a) In paragraphs (a)(ii) and (b)(ii), by deleting “the entry, by” and substituting “in the case of Type 1 surveillance, the entry, by the use of reasonable”.
 - (b) In paragraph (c)(i), in the English text, by deleting “authorization,” and substituting “authorization”.
 - (c) In paragraph (c)(ii), by deleting “the entry, by” and substituting “in the case of Type 1 surveillance, the entry, by the use of reasonable”.
- 30
- (a) In the heading, by deleting “**further**” and substituting “**also**”.
 - (b) By deleting everything before the dash and substituting –
 - “A prescribed authorization also authorizes the undertaking of conduct, including the following conduct, that is necessary for and incidental to the carrying out of what is authorized or required to be carried out under the prescribed authorization”.
- New
- By adding –
- “30A. What a prescribed authorization may not authorize**
- (1) Notwithstanding anything in this

Ordinance, unless exceptional circumstances exist –

- (a) no prescribed authorization may contain terms that authorize the interception of communications by reference to –
 - (i) in the case of a postal interception, an office or other relevant premises, or a residence, of a lawyer; or
 - (ii) in the case of a telecommunications interception, any telecommunications service used at an office or other relevant premises, or a residence, of a lawyer, or any telecommunications service known or reasonably expected to be known by the applicant to be ordinarily used by a lawyer for the purpose of providing legal advice to clients; and
- (b) no prescribed authorization may contain terms that authorize any covert surveillance to be carried out in respect of oral or written communications taking place at an office or other relevant premises, or a residence, of a lawyer.

- (2) For the purposes of subsection (1),

exceptional circumstances exist if the relevant authority is satisfied that there are reasonable grounds to believe –

- (a) that –
 - (i) the lawyer concerned;
 - (ii) in the case of an office or other relevant premises of the lawyer, any other lawyer practising with him or any other person working in the office; or
 - (iii) in the case of a residence of the lawyer, any other person residing in the residence, is a party to any activity which constitutes or would constitute a serious crime or a threat to public security; or
- (b) that any of the communications concerned is for the furtherance of a criminal purpose.

(3) For the avoidance of doubt, a prescribed authorization does not authorize any device to be implanted in, or administered to, a person without the consent of the person.

(4) In this section –
 “lawyer” (律師) means a barrister, solicitor or foreign lawyer as defined in section 2(1) of the Legal Practitioners Ordinance (Cap. 159) who practises as such, or any person holding an appointment under section 3(1) of the Legal Aid Ordinance

(Cap. 91);

“other relevant premises” (其他有關處所), in relation to a lawyer, means any premises, other than an office of the lawyer, that are known or reasonably expected to be known by the applicant to be ordinarily used by the lawyer and by other lawyers for the purpose of providing legal advice to clients.”.

- 36 In the heading, by deleting “**further**” and substituting “**also**”.
- 36(1) (a) By deleting everything before the dash and substituting –
“(1) A device retrieval warrant also authorizes the undertaking of conduct, including the following conduct, that is necessary for and incidental to the carrying out of what is authorized to be carried out under the warrant”.
- (b) In paragraph (b), by adding “the use of reasonable” before “force”.
- 38(3) By deleting “, and may from time to time be reappointed”.
- 38 By adding –
“(5A) A person previously appointed as the Commissioner may from time to time be further appointed as such in accordance with the provisions of this Ordinance that apply to the appointment of the Commissioner.”.
- 39 In paragraph (b), by adding –

“(iia) give notifications to relevant persons under Division 3A;”.

40 By adding –

“(1A) Without limiting the generality of subsection (1), the Commissioner shall conduct reviews on cases in respect of which a report has been submitted to him under section 23(3)(b), 26(3)(b)(ii) or 52.”.

40(2) By adding “or (1A)” after “subsection (1)”.

41(2) By adding “(including any disciplinary action taken in respect of any officer)” before “to address”.

41(3) By deleting everything after “Chief Executive” and substituting “, the Secretary for Justice or any panel judge or any or all of them.”.

42(1) (a) By deleting “believes” and substituting “suspects”.

(b) In paragraphs (a) and (b), by adding “an officer of” before “a department”.

43(1) In paragraph (b), by deleting everything after “whether or not” and substituting “the interception or covert surveillance alleged has been carried out by an officer of a department without the authority of a prescribed authorization issued or renewed under this Ordinance.”.

43(2) By deleting everything after “determines that” and substituting –

“the interception or covert surveillance alleged has been

carried out by an officer of a department without the authority of a prescribed authorization issued or renewed under this Ordinance, he shall as soon as reasonably practicable give notice to the applicant –

- (a) stating that he has found the case in the applicant's favour and indicating whether the case is one of interception or covert surveillance and the duration of the interception or covert surveillance; and
- (b) inviting the applicant to confirm whether the applicant wishes to seek an order for the payment of compensation under the application, and if so, to make written submissions to him for that purpose.”.

43

By adding –

“(2A) Upon receiving confirmation from the applicant that an order for the payment of compensation is sought, the Commissioner, upon taking into account any written submissions made to him for that purpose, may make any order for the payment of compensation by the Government to the applicant.

(2B) The compensation ordered to be paid under subsection (2A) may include compensation for injury of feelings.”.

43(3)

By adding “as soon as reasonably practicable” after “shall”.

43 By deleting subclause (4).

43 By deleting subclause (5) and substituting –

“(5) Notwithstanding subsections (2), (2A) and (3), the Commissioner shall only give a notice or make an order under those subsections when he considers that the giving of the notice or the making of the order (as the case may be) would not be prejudicial to the prevention or detection of crime or the protection of public security.”.

43 By adding –

“(6) The Commissioner shall not make a determination referred to in subsection (2) in respect of an interception if the interception is within the description of section 4(2)(b) or (c).”.

44(1) In paragraph (c), by adding “, after the use of reasonable efforts,” after “cannot”.

45 By deleting subclause (1) and substituting –

“(1) For the purposes of an examination –
 (a) in determining whether any interception or covert surveillance has been carried out without the authority of a prescribed authorization issued or renewed under this Ordinance, the Commissioner shall apply the principles applicable by a court on an application for judicial review;

and

- (b) subject to section 51(1), the Commissioner shall carry out the examination on the basis of written submissions made to him.”.

- 45(3) (a) By deleting “under section 43(2)(a)” and substituting “or making any order under section 43(2), (2A)”.
- (b) In paragraph (b), by deleting “; and” and substituting “further to those mentioned in section 43(2)(a); or”.

- 46(1) (a) By deleting “under” and substituting “referred to in”.
- (b) By adding “, including any order or findings he has made in the examination” before the full stop.

- 46(2) (a) By deleting “notified of the determination” and substituting “given the notification”.
- (b) By adding “(including any disciplinary action taken in respect of any officer)” before “to address”.

- 46(3) By deleting everything after “Chief Executive” and substituting “, the Secretary for Justice or any panel judge or any or all of them.”.

New By adding –

“Division 3A – Notifications by Commissioner

46A. Notifications to relevant persons

- (1) If, in the course of performing any of his functions under this Ordinance, the Commissioner

considers that there is any case in which any interception or covert surveillance has been carried out by an officer of a department without the authority of a prescribed authorization issued or renewed under this Ordinance, subject to subsection (6), the Commissioner shall as soon as reasonably practicable give notice to the relevant person –

- (a) stating that there has been such a case and indicating whether the case is one of interception or covert surveillance and the duration of the interception or covert surveillance; and
- (b) informing the relevant person of his right to apply to the Commissioner for an examination in respect of the interception or covert surveillance.

(2) Where the relevant person makes an application for an examination in respect of the interception or covert surveillance within 6 months after receipt of the notice or within such further period as the Commissioner may allow, the Commissioner shall, notwithstanding anything in section 44(1)(a) but subject to the other provisions of section 44, make a determination referred to in section 43(2), and the provisions of this Ordinance are to apply accordingly.

(3) Notwithstanding subsection (1), the Commissioner shall only give a notice under that subsection when he considers that the giving of the notice would not be prejudicial to the prevention or detection of crime or the protection of public security.

(4) Without prejudice to subsection (3), in giving notice to a relevant person under subsection (1), the Commissioner shall not –

- (a) give reasons for his findings; or
- (b) give details of any interception or covert surveillance concerned further to those mentioned in subsection (1)(a).

(5) For the purposes of this section, in considering whether any interception or covert surveillance has been carried out without the authority of a prescribed authorization issued or renewed under this Ordinance, the Commissioner shall apply the principles applicable by a court on an application for judicial review.

(6) This section does not require the Commissioner to give any notice to a relevant person if –

- (a) the relevant person cannot, after the use of reasonable efforts, be identified or traced;
- (b) the Commissioner considers that the intrusiveness of the interception or covert surveillance concerned on the relevant person is negligible; or
- (c) in the case of interception, the interception is within the description of section 4(2)(b) or (c).

(7) In this section, “relevant person” (有關人士) means any person who is the subject of the interception or covert surveillance concerned.”.

47(2)

- (a) By deleting paragraph (a) and substituting –
- “(a) a list showing –
- (i) the respective numbers of judge’s authorizations, executive authorizations and emergency authorizations issued under this Ordinance during the report period, and the average duration of the respective prescribed authorizations;
 - (ii) the respective numbers of judge’s authorizations and executive authorizations renewed under this Ordinance during the report period, and the average duration of the respective renewals;
 - (iii) the respective numbers of judge’s authorizations, executive authorizations and emergency authorizations issued as a result of an oral application under this Ordinance during the report period, and the average duration of the respective prescribed authorizations;
 - (iv) the respective numbers of judge’s authorizations and executive authorizations renewed as a result of an oral application under this Ordinance during the report period, and the average duration of the respective renewals;
 - (v) the respective numbers of judge’s authorizations and executive authorizations that have been renewed under this Ordinance during the report period further

- to 5 or more previous renewals;
 - (vi) the respective numbers of applications for the issue of judge's authorizations, executive authorizations and emergency authorizations made under this Ordinance that have been refused during the report period;
 - (vii) the respective numbers of applications for the renewal of judge's authorizations and executive authorizations made under this Ordinance that have been refused during the report period;
 - (viii) the respective numbers of oral applications for the issue of judge's authorizations, executive authorizations and emergency authorizations made under this Ordinance that have been refused during the report period; and
 - (ix) the respective numbers of oral applications for the renewal of judge's authorizations and executive authorizations made under this Ordinance that have been refused during the report period;".
- (b) In paragraph (d)(ii), by adding "or errors" after "irregularities".
 - (c) By deleting paragraph (d)(iv) and substituting –
 - "(iv) the respective numbers of notices given by the Commissioner under section 43(2) and section 43(3) during the report period further to examinations;".
 - (d) In paragraph (d), by adding –

“(iva) the number of cases in which a notice has been given by the Commissioner under section 46A during the report period;”.

(e) In paragraph (d)(v), by adding “48,” before “49”.

(f) In paragraph (d)(v), by deleting “and” at the end.

(g) In paragraph (d), by adding –

“(vi) the number of cases in which information subject to legal professional privilege has been obtained in consequence of any interception or covert surveillance carried out pursuant to a prescribed authorization during the report period; and

(vii) the number of cases in which disciplinary action has been taken in respect of any officer of a department according to any report submitted to the Commissioner under section 41, 46, 50 or 52 during the report period, and the broad nature of such action; and”.

47

By deleting subclause (4) and substituting –

“(4) The Chief Executive shall cause to be laid on the table of the Legislative Council a copy of the report, together with a statement as to whether any matter has been excluded from that copy under subsection (5) without the agreement of the Commissioner.”.

50(2)

By adding “(including any disciplinary action taken in respect of any officer)” before “to implement”.

50(3)

By deleting everything after “Chief Executive” and substituting “, the Secretary for Justice or any panel judge or any or all of

them.”.

51

By adding –

“(1A) For the purpose of performing any of his functions under this Ordinance, the Commissioner may request a panel judge to provide him with access to any of the documents or records kept under section 3 of Schedule 2.”.

52

By adding “(including any disciplinary action taken in respect of any officer)” before the full stop.

55(1)

By deleting everything before “ground” and substituting –

“(1) If the officer by whom any regular review is or has been conducted under section 54(1) or (2) is of the opinion that the”.

55(2)

- (a) In paragraph (a), in the English text, by deleting “any ground” and substituting “the ground”.
- (b) In the Chinese text, by adding “有關部門” before “在當其時”.
- (c) In the Chinese text, by deleting “有關部門的人員” and substituting “人員”.

55

By adding –

“(5A) If, at the time of the provision of a report to the relevant authority under subsection (3), the relevant authority is no longer holding his office or performing the relevant functions of his office –

- (a) without prejudice to section 54 of

the Interpretation and General
 Clauses Ordinance (Cap. 1), the
 reference to relevant authority in
 that subsection includes the person
 for the time being appointed as a
 panel judge or authorizing officer
 (as the case may be) and lawfully
 performing the relevant functions of
 the office of that relevant authority;
 and

- (b) the provisions of this section are to
 apply accordingly.”.

55 By deleting subclause (6) and substituting –

“(6) For the purposes of this section, the ground
 for discontinuance of a prescribed authorization exists if
 the conditions for the continuance of the prescribed
 authorization under section 3 are not met.”.

New By adding –

**“55A. Reports to relevant authorities
 following arrests**

(1) Where, further to the issue or renewal of a
 prescribed authorization under this Ordinance, the
 officer of the department concerned who is for the time
 being in charge of the interception or covert surveillance
 concerned becomes aware that the subject of the
 interception or covert surveillance has been arrested, the
 officer shall, as soon as reasonably practicable after he
 becomes aware of the matter, cause to be provided to the
 relevant authority by whom the prescribed authorization

has been issued or renewed a report assessing the effect of the arrest on the likelihood that any information which may be subject to legal professional privilege will be obtained by continuing the interception or covert surveillance.

(2) Where the relevant authority receives a report under subsection (1), he shall revoke the prescribed authorization if he considers that the conditions for the continuance of the prescribed authorization under section 3 are not met.

(3) Where the prescribed authorization is revoked under subsection (2), the prescribed authorization is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.

(4) If, at the time of the provision of a report to the relevant authority under subsection (1), the relevant authority is no longer holding his office or performing the relevant functions of his office –

(a) without prejudice to section 54 of the Interpretation and General Clauses Ordinance (Cap. 1), the reference to relevant authority in that subsection includes the person for the time being appointed as a panel judge or authorizing officer (as the case may be) and lawfully performing the relevant functions of the office of that relevant authority; and

(b) the provisions of this section are to

apply accordingly.

(5) In this section, “relevant duration provision” (有關時限條文) means section 10(*b*), 13(*b*), 16(*b*), 19(*b*) or 22(1)(*b*) (as may be applicable).”.

56

By adding –

“(1A) Where any protected product described in subsection (1) contains any information that is subject to legal professional privilege, subsection (1)(*c*) is to be construed as also requiring the head of the department concerned to make arrangements to ensure that any part of the protected product that contains the information –

- (*a*) in the case of a prescribed authorization for a postal interception or covert surveillance, is destroyed not later than 1 year after its retention ceases to be necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted; or
- (*b*) in the case of a prescribed authorization for a telecommunications interception, is as soon as reasonably practicable destroyed.”.

56

By deleting subclause (2) and substituting –

“(2) For the purposes of this section, something is necessary for the relevant purpose of a prescribed

authorization –

- (a) in the case of subsection (1)(a), if –
 - (i) it continues to be, or is likely to become, necessary for the relevant purpose; or
 - (ii) except in the case of a prescribed authorization for a telecommunications interception, it is necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted; or
- (b) in the case of subsection (1)(c) –
 - (i) when it continues to be, or is likely to become, necessary for the relevant purpose; or
 - (ii) except in the case of a prescribed authorization for a telecommunications interception, at any time before the expiration of 1 year after it ceases to be necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted.”.

57(2)

- (a) In paragraph (a)(ii)(A), by deleting everything after

“application,” and substituting “for a period of at least 1 year after the pending proceedings, review or application has been finally determined or finally disposed of; or”.

- (b) In paragraph (a)(ii)(B), by deleting “at least until” and substituting “for a period of at least 1 year after”.
- (c) In paragraph (a)(ii)(B), by deleting “, until” and substituting “, for a period of at least 1 year after”.

58

By deleting subclause (4) and substituting –

“(4) Notwithstanding subsection (2), where, for the purposes of any criminal proceedings (whether being criminal proceedings instituted for an offence or any related proceedings), any information obtained pursuant to a relevant prescribed authorization and continuing to be available to the department concerned might reasonably be considered capable of undermining the case for the prosecution against the defence or of assisting the case for the defence –

- (a) the department shall disclose the information to the prosecution; and
- (b) the prosecution shall then disclose the information to the judge in an ex parte hearing that is held in private.”.

58

By deleting subclause (5).

58

By deleting subclause (6) and substituting –

“(6) The judge may, further to the disclosure to him of the information under subsection (4)(b), make such orders as he thinks fit for the purpose of securing

the fairness of the proceedings.”.

58

By adding –

“(6A) Where any order is made under subsection (6) in any criminal proceedings, the prosecution shall disclose to the judge for any related proceedings the terms of the order and the information concerned in an ex parte hearing that is held in private.”.

58(7)

By deleting “direction” and substituting “order”.

58(8)

By adding –

““judge” (法官), in relation to any proceedings, means the judge or magistrate before whom those proceedings are or are to be heard, or any other judge or magistrate having jurisdiction to deal with the matter concerned;

“related proceedings” (有關法律程序), in relation to any criminal proceedings, means any further proceedings (including appeal proceedings) arising from, or any proceedings preliminary or incidental to, those proceedings;”.

New

By adding –

“58A. Information subject to legal professional privilege to remain privileged

Any information that is subject to legal professional privilege is to remain privileged notwithstanding that it has been obtained pursuant to a prescribed authorization.”.

- 59(4) By deleting “have regard to” and substituting “comply with”.
- 60(1) By deleting “in” and substituting “relating to”.
- 60(2) (a) By deleting “prejudice to” and substituting “limiting”.
 (b) By deleting “defect in” and substituting “defect relating to”.
- 62 By deleting “make regulation” and substituting “, subject to the approval of the Legislative Council, make regulations”.
- 63 By deleting everything after “may,” and substituting “subject to the approval of the Legislative Council, amend Schedules 1, 2, 3 and 4 by notice published in the Gazette.”.
- 65(1) (a) By deleting “the provision then in force as”.
 (b) By deleting “sections 56 and 58 apply” and substituting “section 56 applies”.
 (c) By deleting “and to the relevant matters”.
 (d) By deleting paragraph (a)(i) and substituting –
 “(i) the materials were protected product; and”.
- 65 By adding –
 “(2A) Nothing in this section operates to validate or authorize any telecommunications interception carried out pursuant to an order referred to in subsection (1).”.
- 65 By deleting subclause (3) and substituting –
 “(3) In this section, “copy” (文本), in relation

to any contents of a communication referred to in subsection (1), means any of the following (whether or not in documentary form) –

- (a) any copy, extract or summary of such contents;
- (b) any record referring to the telecommunications interception referred to in subsection (1) which is a record showing, directly or indirectly, the identity of any person who is the sender or intended recipient of the communication.”.

Schedule 2	Within the square brackets, by deleting “2, 6” and substituting “6, 51”.
Schedule 2, section 1(2)	By deleting everything after “considered” and substituting “outside the court precincts at any place other than the premises of a department.”.
Schedule 2, section 1	By deleting subsection (3) and substituting – “(3) The panel judge may consider the application in such manner as he considers appropriate.”.
Schedule 2, section 3(3)	In paragraph (b), by adding “(including those performed at the request of the Commissioner under section 51(1A) of this Ordinance)” before “; and”.
Schedule 2, section 3(5)	(a) In the English text, by adding “, whether” after “department concerned”. (b) By deleting “otherwise”.

Schedule 2,
section 4

By deleting the section.

Schedule 3,
Part 1

- (a) In paragraph (b)(v), by deleting “nature of, and an assessment of the immediacy and gravity of” and substituting “following information”.
- (b) In paragraph (b)(v)(A), by adding “nature of, and an assessment of the immediacy and gravity of, the particular” before “serious”.
- (c) By deleting paragraph (b)(v)(B) and substituting –
 - “(B) where the purpose sought to be furthered by carrying out the interception is that specified in section 3(1)(a)(ii) of this Ordinance, the nature of, and an assessment of the immediacy and gravity of, the particular threat to public security, and an assessment of the impact, both direct and indirect, of the threat on the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong;”.
- (d) In paragraph (b)(viii), by adding “, or may be the contents of any journalistic material,” after “privilege”.
- (e) In paragraph (b)(viii), by deleting “and”.
- (f) In paragraph (b), by adding –
 - “(x) if known, whether, during the preceding 2 years, there has been any application for the issue or renewal of a prescribed authorization in which –
 - (A) any person set out in the affidavit under subparagraph (ii) has also been identified as the subject of the interception or covert surveillance concerned; or

- (B) where the particulars of any telecommunications service have been set out in the affidavit under subparagraph (iii), the interception of any communication to or from that telecommunications service has also been sought,
 - and if so, particulars of such application; and”.
 - (g) In paragraph (c), by deleting everything after “name” and substituting “, rank and post the applicant and any officer of the department concerned approving the making of the application.”.
- Schedule 3,
Part 2
- (a) In paragraph (b)(vi), by deleting “nature of, and an assessment of the immediacy and gravity of” and substituting “following information”.
 - (b) In paragraph (b)(vi)(A), by adding “nature of, and an assessment of the immediacy and gravity of, the particular” before “serious”.
 - (c) By deleting paragraph (b)(vi)(B) and substituting –
 - “(B) where the purpose sought to be furthered by carrying out the Type 1 surveillance is that specified in section 3(1)(a)(ii) of this Ordinance, the nature of, and an assessment of the immediacy and gravity of, the particular threat to public security, and an assessment of the impact, both direct and indirect, of the threat on the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong;”.
 - (d) In paragraph (b)(ix), by adding “, or may be the contents of any journalistic material,” after “privilege”.

- (e) In paragraph (b)(ix), by deleting “and”.
- (f) In paragraph (b), by adding –
 - “(xi) if known, whether, during the preceding 2 years, there has been any application for the issue or renewal of a prescribed authorization in which any person set out in the affidavit under subparagraph (ii) has also been identified as the subject of the interception or covert surveillance concerned, and if so, particulars of such application; and”.
- (g) In paragraph (c), by deleting everything after “name” and substituting “, rank and post the applicant and any officer of the department concerned approving the making of the application.”.

Schedule 3,
Part 3

- (a) In paragraph (b)(vi), by deleting “nature of, and an assessment of the immediacy and gravity of” and substituting “following information”.
- (b) In paragraph (b)(vi)(A), by adding “nature of, and an assessment of the immediacy and gravity of, the particular” before “serious”.
- (c) By deleting paragraph (b)(vi)(B) and substituting –
 - “(B) where the purpose sought to be furthered by carrying out the Type 2 surveillance is that specified in section 3(1)(a)(ii) of this Ordinance, the nature of, and an assessment of the immediacy and gravity of, the particular threat to public security, and an assessment of the impact, both direct and indirect, of the threat on the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong;”.

- (d) In paragraph (b)(ix), by adding “, or may be the contents of any journalistic material,” after “privilege”.
- (e) In paragraph (b)(ix), by deleting “and”.
- (f) In paragraph (b), by adding –
 - “(xi) if known, whether, during the preceding 2 years, there has been any application for the issue or renewal of a prescribed authorization in which any person set out in the statement under subparagraph (ii) has also been identified as the subject of the interception or covert surveillance concerned, and if so, particulars of such application; and”.
- (g) In paragraph (c), by deleting “and rank” and substituting “, rank and post”.

Schedule 3,
Part 4

- (a) In paragraph (a)(iii), by adding “an assessment of” before “the value”.
- (b) In paragraph (b), by deleting everything after “name” and substituting “, rank and post the applicant and any officer of the department concerned approving the making of the application.”.

Schedule 4

In paragraph (b), by deleting “and rank” and substituting “, rank and post”.

2(1) (definition of “prescribed authorization” and paragraph (a) of the definition of “relevant authority”), 8(1) and (2)(b), 9(1),

By deleting “judicial authorization” wherever it appears and substituting “judge’s authorization”.

(2) and (3)(a),
 10, 11(1) and
 (2)(b)(i) and (ii),
 12(1), (3)(a) and
 (4), 13, 20(1)(b)
 and 22(2) and
 Schedule 3 (Parts
 1, 2 and 4)

Part 3	In the heading of Division 2, by deleting “ Judicial Authorizations ” and substituting “ Judge’s Authorizations ”.
8 and 11	In the cross-headings immediately before the clauses, by deleting “ <i>judicial authorizations</i> ” and substituting “ <i>judge’s authorizations</i> ”.
8, 9, 10, 11, 12 and 13	In the headings, by deleting “ judicial authorization ” and substituting “ judge’s authorization ”.
Schedule 3 (Parts 1, 2 and 4)	In the headings, by deleting “JUDICIAL AUTHORIZATION” and substituting “JUDGE’S AUTHORIZATION”.

INTERCEPTION OF COMMUNICATIONS AND SURVEILLANCE BILL

Committee Stage Amendments proposed by Hon. Margaret Ng

CONTENTS

Clause Page PART 1

PRELIMINARY

1. Short title..... C155
2. Interpretation C155
3. Conditions for issue, renewal or continuance of prescribed
authorization..... C169

PART 2

PROHIBITION ON INTERCEPTION AND COVERT SURVEILLANCE

4. Prohibition on interception C171
5. Prohibition on covert surveillance C171

PART 3

PRESCRIBED AUTHORIZATIONS, ETC.

Division 1—Relevant Authorities

6. Panel judge Courts C173
7. Authorizing officers C173

Division 2—Judicial Authorizations

Issue of judicial authorizations

- 8. Application for judicial authorization for interception or Type 1 surveillance C173
- 9. Determination of application for judicial authorization C175
- 10. Duration of judicial authorization..... C175

Renewal of judicial authorizations

- 11. Application for renewal of judicial authorization C175
- 12. Determination of application for renewal of judicial authorization C177
- 13. Duration of renewal of judicial authorization C177

Division 3—Executive Authorizations

Issue of executive authorizations

- 14. Application for executive authorization for Type 2 surveillance C179
- 15. Determination of application for executive authorization C179
- 16. Duration of executive authorization C179

Renewal of executive authorizations

- 17. Application for renewal of executive authorization C181
- 18. Determination of application for renewal of executive authorization..... C181
- 19. Duration of renewal of executive authorization C183

Division 4—Emergency Authorizations

Issue of emergency authorizations

20. Application for emergency authorization for interception or Type 1 surveillance in case of emergency C183
21. Determination of application for emergency authorization C185
22. Duration of emergency authorization C185

Application for confirmation of emergency authorizations

23. Application for confirmation of emergency authorization C187
24. Determination of application for confirmation of emergency authorization C187

Division 5—Special Provisions for Oral Applications

Oral applications

25. Oral application and its effect C189

Application for confirmation of prescribed authorizations or renewals issued or granted upon oral applications

26. Application for confirmation of prescribed authorization or renewal issued or granted upon oral application C191
27. Determination of application for confirmation of prescribed authorization or renewal issued or granted upon oral application C195
28. Special case of emergency authorization issued as a result of oral application C197

Division 6—General Provisions for Prescribed Authorizations

Matters authorized, required or provided for by prescribed authorizations

- 29. What a prescribed authorization may authorize or require under or by virtue of its terms, etc. C199
- 30. What a prescribed authorization further authorizes C203
- 31. Prescribed authorization may be issued or renewed subject to conditions C205

Device retrieval warrants after prescribed authorizations having ceased to have effect

- 32. Application for device retrieval warrant C205
- 33. Determination of application for device retrieval warrant C207
- 34. Duration of device retrieval warrant C207
- 35. What a device retrieval warrant may authorize under or by virtue of its terms, etc. C207
- 36. What a device retrieval warrant further authorizes C209
- 37. Device retrieval warrant may be issued subject to conditions C209

PART 4

THE COMMISSIONER

Division 1—The Commissioner and his Functions

38. The Commissioner C209
39. Functions of Commissioner C211

Division 2—Reviews by Commissioner

40. Reviews on compliance with relevant requirements C211
41. Notifications to departments concerned, etc. C213

Division 3—Examinations by Commissioner

42. Application for examination C213
43. Examination by Commissioner C213
44. Grounds for not carrying out examination, etc. C215
45. Further provisions relating to examinations .. C217
46. Notifications to departments concerned, etc. C217

Division 4—Reports and Recommendations by Commissioner

47. Annual reports to Chief Executive by Commissioner C219
48. Other reports to Chief Executive by Commissioner C221
49. Recommendations to Secretary for Security on code of practice C221
50. Recommendations to departments C223

Division 5—Further Provisions Relating to Performance of Functions by Commissioner

51. Further powers of Commissioner C223

52. General obligations of departments to report on noncompliance C225
53. Commissioner not regarded as court C225

PART 5 FURTHER SAFEGUARDS

54. Regular reviews C225
55. Discontinuance of interception or covert surveillance C227
56. Safeguards for protected products C229
57. Record keeping C229
58. Non-admissibility of telecommunications interception product C235
59. Code of practice C237

PART 6 MISCELLANEOUS

60. Prescribed authorizations and device retrieval warrants not affected by minor defects C239
61. Immunity C239
62. Regulation C241
63. Amendment of Schedules C241
64. Repeal and consequential amendments C241
65. Transitional arrangements C241
- Schedule 1 Departments C245
- Schedule 2 Procedures of, and other matters relating to, panel judge~~court~~ C245
- Schedule 3 Requirements for affidavit or statement for application for issue or renewal of prescribed authorization for interception or covert surveillance C249

Schedule 4 Requirements for affidavit for application for issue of
device retrieval warrant C257

Schedule 5 Consequential amendments C259

A BILL To

Regulate the conduct of interception of communications and the
use of surveillance devices by or on behalf of public officers and to
provide for related matters.

Enacted by the Legislative Council.

PART 1

PRELIMINARY

1. Short title

This Ordinance may be cited as the Interception of
Communications and Surveillance Ordinance.

2. Interpretation

(1) In this Ordinance, unless the context otherwise requires—
“address” (地址), in relation to a communication transmitted by a
postal service, includes a postal box address;

“authorizing officer” (授權人員), in relation to any department,
means any officer designated under section 7 by the head of the
department to be an
authorizing officer;

“code of practice” (實務守則) means the code of practice issued
under section 59;

“Commissioner” (專員) means the Commissioner on Interception
of Communications and Surveillance appointed under section 38;

“communication” (通訊) means—

~~(a) any communication transmitted by a postal service; or~~
~~(b) any communication transmitted by a telecommunications system;~~

communication transmitted by any means whatsoever including by a postal or courier service or telecommunications system

“communication transmitted by a postal service” (藉郵政服務傳送的通訊) includes a postal article;

“conduct” (行爲) includes any act or omission, and any series of acts or omissions or of acts and omissions;

“conveyance” (運輸工具) means any vehicle, vessel, aircraft, hovercraft or other conveyance;

“copy” (文本)—

(a) in relation to any contents of a communication that have been obtained pursuant to a prescribed authorization for interception, means any of the following (whether or not in documentary form)—

(i) any copy, extract or summary of such contents which identifies itself as such copy, extract or summary of such contents;

(ii) any record referring to the interception which is a record of the identity of any person who is the sender or intended recipient of the communication; or

(b) in relation to any material that has been obtained pursuant to a prescribed authorization for covert surveillance, means any of the following (whether or not in documentary form)—

(i) any copy, extract or summary of the material which identifies itself as such copy, extract or summary of the material;

(ii) any transcript or record made of the material which identifies itself as such transcript or record made of the material;

“court” (法院), without prejudice to section 53 and section 4 of Schedule 2—

(a) means a court as defined in section 3 of the Interpretation and General Clauses Ordinance (Cap. 1); and

(b) includes a magistrate and a tribunal;

“covert surveillance” (秘密監察)—

(a) means any ~~systematic~~ surveillance carried out with the use of any surveillance device or by an undercover agent of a department specified in Schedule 1 for the purposes of a specific investigation or operation, if the surveillance—

~~(i) is carried out in circumstances where any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy;~~

(ii) ~~(i)~~ is carried out in a manner calculated to ensure that the person is unaware that the surveillance is or may be taking place; and

(iii) ~~(ii)~~ is likely to result in the obtaining of any private information about the person; but

(b) does not include any such ~~systematic~~ surveillance ~~to the extent~~ that it constitutes interception under this Ordinance;

“data surveillance device” (數據監察器材)—

(a) means any device or program used to monitor or record the input of information into, or the output of information from, any information system; but

(b) does not include an optical surveillance device;

“department” (部門)—

(a) in relation to interception (including any application for the issue or renewal of a prescribed authorization for interception, any prescribed authorization for interception and any other matter relating to interception), means a department specified in Part 1 of Schedule 1;

(b) in relation to covert surveillance (including any application for the issue or renewal of a prescribed authorization for covert

surveillance, any prescribed authorization for covert surveillance and any other matter relating to covert surveillance), means a department specified in Part 2 of Schedule 1; or

(c) in relation to any other matter provided for in this Ordinance, means a department specified in Part 1 or 2 of Schedule 1;

“device” (器材) includes any instrument, apparatus and equipment;

“device retrieval warrant” (器材取出手令) means a device retrieval warrant issued under section 33 (and, where the context requires, includes a device retrieval warrant to be issued under that section);

“directorate officer” (首長級人員) means an officer not below a rank equivalent to that of chief superintendent of police;

“emergency authorization” (緊急授權) means an emergency authorization issued under Division 4 of Part 3 (and, where the context requires, includes an emergency authorization to be issued under that Division);

“enhancement equipment” (增強設備), in relation to a device, means any equipment used to enhance a signal, image or other information obtained by the use of the device;

“examination” (審查) means an examination (including consideration of the application for the examination) carried out under Division 3 of Part 4 (and, where the context requires, includes such an examination to be carried out under that Division);

“executive authorization” (行政授權) means an executive authorization issued or renewed under Division 3 of Part 3 (and, where the context requires, includes an executive authorization to be issued or renewed under that Division);

“function” (職能) includes power and duty;

“head” (首長), in relation to a department, includes any deputy of the head of the department;

“information system” (資訊系統) has the meaning assigned to it by section 2(1) of the Electronic Transactions Ordinance (Cap. 553);

“inspect” (查察) includes listen to, monitor and record;

“install” (裝設) includes attach;

“intercepting act” (截取作為), in relation to any communication, means the inspection of some or all of the contents of the communication, ~~in the course of its transmission by a postal service or by a telecommunications system,~~

(i) by a person other than its sender or intended recipient or
(ii) by a recipient who is an undercover agent of a department specified in Schedule 1;

“interception” (截取)—

(a) in relation to any communication, means the carrying out of any intercepting act in respect of the communication; or

(b) when appearing in a context with no specific reference to any communication, means the carrying out of any intercepting act in respect of communications;

“interception product” (截取成果) means any contents of a communication that have been obtained pursuant to ~~a prescribed authorization for an~~ interception, and includes a copy of such contents;

“judicial authorization” (司法授權) means a judicial authorization issued or renewed under Division 2 of Part 3 (and, where the context requires, includes a judicial authorization to be issued or renewed under that Division);

“listening device” (監聽器材)—

(a) means any device used to overhear, listen to, monitor or record any conversation or words spoken to or by any person in conversation; but

(b) does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment;

“maintain” (維修), in relation to a device, includes—

(a) adjust, relocate, repair or service the device; and

(b) replace the device when it is faulty;

“optical surveillance device” (視光監察器材)—

(a) means any device used to record visually or observe any activity; but

(b) does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome the impairment;

~~“oral application” (口頭申請) means an oral application made under section 25(1);~~

“panel judge” (小組法官) means a judge appointed under section 6(1) to be a panel judge;

“postal interception” (郵件截取) means interception of any communication transmitted by a postal service;

“postal service” (郵政服務) means any communication service including a postal service within the meaning of the Post Office Ordinance (Cap. 98);

“premises” (處所) includes any place and, in particular, includes—

(a) any land or building;

(b) any conveyance;

(c) any structure (whether or not movable or offshore); and

(d) any part of any of the premises described in paragraph (a), (b) or (c);

“prescribed authorization” (訂明授權) means a judicial authorization, an executive authorization or an emergency authorization;

“protected product” (受保護成果) means any interception product or surveillance product and includes any information derived from such product and any document or record containing such information

“public place” (公眾地方)—

(a) means any premises which are a public place as defined in section 2(1) of the Summary Offences Ordinance (Cap. 228); but

(b) does not include any such premises ~~to the extent that they~~ are intended for use by members of the public as a lavatory or as a place for taking a bath or changing clothes;

“public security” (公共安全) means the public security of Hong Kong from terrorist acts which present a clear and imminent threat to life or by acts immediately endangering public safety

“relevant authority” (有關當局)—

(a) in relation to an application for the issue or renewal of a judicial judge’ s authorization, means the panel judge to whom the application is or has been made;

(b) in relation to an application for the issue or renewal of an executive authorization, means the authorizing officer to whom the application is or has been made; or

(c) in relation to an application for the issue of an emergency authorization, means the head of a department to whom the application is or has been made;

“relevant purpose” (有關目的), in relation to a prescribed authorization, means the purpose sought to be furthered by carrying out the interception or covert surveillance concerned as described in section 3 for the purpose of the issue or renewal, or the continuance, of the prescribed authorization;

“relevant requirement” (有關規定) means any applicable requirement under—

(a) any provision of this Ordinance;

(b) the code of practice; or

(c) any prescribed authorization or device retrieval warrant concerned;

“serious crime” (嚴重罪行) means any offence punishable—

~~(a) in relation to the issue or renewal, or the continuance, of a prescribed authorization for interception, by a maximum penalty that is or includes a term of imprisonment of not less than 7 years~~
or

~~(b) in relation to the issue or renewal, or the continuance, of a prescribed authorization for covert surveillance, by a maximum penalty that is or includes—~~

~~(i) a term of imprisonment of not less than 3 years; or~~

~~(ii) a fine of not less than \$1,000,000;~~

“subject of interception or surveillance” means any person whose activity is being monitored by interception of his communication or surveillance;

“surveillance device” (監察器材) means—

- (a) a data surveillance device, a listening device, an optical surveillance device or a tracking device;
- (b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a); or
- (c) a device of a class prescribed by regulation made under section 62 for the purposes of this definition;

“surveillance product” (監察成果) means any material obtained pursuant to ~~a prescribed authorization for~~ covert surveillance, and includes a copy of the material, any information derived from the material, and any odcumetn or record containing such information;

“telecommunications interception” (電訊截取) means interception of any communication transmitted by a telecommunications system;

“telecommunications service” (電訊服務) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

“telecommunications system” (電訊系統) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

“tracking device” (追蹤系統) means any electronic device used to determine or monitor the location of any person or any object or the status of any object;

“transmitted” (傳送) includes being transmitted;

“Type 1 surveillance” (第 1 類監察) means any covert surveillance ~~other than Type 2 surveillance~~ which is

- (a) carried out with the use of any surveillance or tracking device; or
- (b) involves entry onto any premises without permission; or
- (c) interferes with the interior of any conveyance or object without permission

“Type 2 surveillance” (第 2 類監察), subject to subsection (3), means any covert surveillance other than Type 1 surveillance to the extent that—

(a) it is carried out with the use of a surveillance device for any purpose involving listening to, monitoring or recording words spoken or activity carried out by any person, and the person using the device is one—

(i) who—

(A) is the person speaking or carrying out the words or activity; or

(B) is a person, or is included in a class of persons, by whom the person described in sub-paragraph (A) intends, or should reasonably expect, the words or activity to be heard or seen; or

(ii) who listens to, monitors or records the words or activity with the consent, express or implied, of a person described in subparagraph (i)(A) or (B); or

(b) it is carried out with the use of an optical surveillance device or a tracking device and the use of the device does not involve—

(i) entry onto any premises without permission; or

(ii) interference with the interior of any conveyance or object without permission.

(2) For the purposes of this Ordinance, a person is not regarded as being entitled to a reasonable expectation of privacy within the meaning of paragraph (a)(i) of the definition of “covert surveillance” in subsection (1) in relation to any activity carried out by him in a public place

(3) For the purposes of this Ordinance, any covert surveillance which is Type 2 surveillance under the definition of “Type 2 surveillance” in subsection (1) is regarded as Type 1 surveillance if it is likely that any information which may be subject to legal professional privilege will be obtained by carrying it out.

(4) For the purposes of this Ordinance—

~~(a) a communication transmitted by a postal service is regarded as being in the course of the transmission if it is regarded as being in course of transmission by post under section 2(2) of the Post Office Ordinance (Cap. 98); and~~

~~(b) a communication transmitted by a telecommunications system is not regarded as being in the course of the transmission if it has been received by the intended recipient of the communication or by an information system or facility under his control or to which he may have access, whether or not he has actually read or listened to the contents of the communication.~~

(5) For the purposes of this Ordinance, the contents of any communication transmitted by a telecommunications system include any data produced in association with the communication.

(5A) For the purposes of this Ordinance, the exercise of any right enjoyed by any person under the Basic Law or under international treaties, conventions or instruments applying to the HKSAR or under common law shall not be regarded as a threat to public security

~~(6) For the purposes of this Ordinance—~~

~~(a) an application is also regarded as being made orally if it is made by telephone, video conferencing or other electronic means by which words spoken can be heard (whether or not any part of the application is made in writing);~~

~~(b) information is also regarded as being provided orally if it is provided by telephone, video conferencing or other electronic means by which words spoken can be heard (whether or not any part of the information is provided in writing); and~~

~~(c) a determination (including the issue of a prescribed authorization or a renewed prescribed authorization and the giving of any reason) is also regarded as being delivered orally if it is delivered by telephone, video conferencing or other electronic means by which words spoken can be heard (whether or not any part of the determination is delivered in writing).~~

~~(7) Without prejudice to section 54 of the Interpretation and General Clauses Ordinance (Cap. 1), any reference in this~~

~~Ordinance to a panel judge or any officer of a department (however expressed) includes—~~

~~(a) where the person who has been such panel judge or officer is no longer holding office as such panel judge or officer, the person for the time being holding such office or appointed to act in or perform the functions of such office or lawfully performing the functions of such office; or~~

~~(b) where the person who is such panel judge or officer is unable to perform the functions of the office of such panel judge or officer, the person for the time being appointed to act in or perform the functions of such office or lawfully performing the functions of such office.~~

3. Conditions for issue, renewal or continuance of prescribed authorization

(1) In this Ordinance, the conditions for the issue or renewal, or the continuance, of a prescribed authorization, are that, in the circumstances of the particular case—

(a) the purpose of sought to be furthered by carrying out the interception or covert surveillance concerned is that of—

(i) preventing or detecting a serious crime which the applicant reasonably believes is about to take place or has taken place as the case may be; or

(ii) protecting public security against a threat which the applicant reasonably believes to be imminent;

(aa) there is credible evidence to show a reasonable suspicion that the subject of the interception or covert surveillance has been, is, or is likely to be, involved in—

(i) Committing the serious crime; or

(ii) undertaking the activity which constitutes or would constitute a threat to public security; and

(b) the serious crime to be prevented or detected or the particular threat to public security referred to in (a)(i) and (ii) as the case may be is identified

(c) ~~(b)~~ the interception or covert surveillance is ~~proportionate to the purpose sought to be furthered by carrying it out~~, in all

circumstances, necessary and proportionate to the purpose, upon—

- (i) balancing, ~~in operational terms~~, the relevant factors against the intrusiveness of the interception or covert surveillance on any person who is to be the subject of or may be affected by the interception or covert surveillance; and
- (ii) considering whether the purpose sought to be furthered by carrying out the interception or covert surveillance can reasonably be furthered by other less intrusive means.

(2) In this section, “relevant factors” (有關因素) means—

(a) the right to freedom and privacy protected by article 30 of the Basic Law;

(ba) the rights and freedoms protected in the Basic Law and the International Covenant on Civil and Political Rights

(cb) the immediacy and gravity of—

- (i) where the purpose sought to be furthered by carrying out the interception or covert surveillance concerned is that specified in subsection (1)(a)(i), the serious crime to be prevented or detected; or
- (ii) where the purpose sought to be furthered by carrying out the interception or covert surveillance concerned is that specified in subsection (1)(a)(ii), the particular threat to public security; and

(bd) the likely value and relevance, in relation to the purpose ~~sought to be furthered~~ of by carrying out the interception or covert surveillance, of the information likely to be obtained by carrying it out.

PART 2

PROHIBITION ON INTERCEPTION AND COVERT SURVEILLANCE

4. Prohibition on interception

(1) Subject to subsection (2), neither the Chief Executive, members of the Executive Council, bureau heads insofar as they are not public servants nor any public officer shall, directly or through any other person, carry out any interception.

(2) Subsection (1) does not apply to—

(a) any interception carried out pursuant to a prescribed authorization;

~~(b) any interception of telecommunications transmitted by radiocommunications (other than the radiocommunications part of a telecommunications network for the provision of a public telecommunications service by any carrier licensee under the Telecommunications Ordinance (Cap. 106)); and~~

(c) any interception authorized, permitted or required to be carried out by or under any enactment other than this Ordinance ~~(including any interception carried out in the course of the execution of an order of a court authorizing the search of any premises or the seizure of any evidence).~~

(3) ~~In this section, “carrier licensee” (傳送者牌照持有人), “public telecommunications service” (公共電訊服務), “radiocommunications” (無線電通訊), “telecommunications” (電訊) and “telecommunications network” (電訊網絡) have the meanings respectively assigned to them by section 2(1) of the Telecommunications Ordinance (Cap. 106).~~

5. Prohibition on covert surveillance

(1) Subject to subsection (2), neither the Chief Executive, members of the Executive Council, bureau heads insofar as they are not public servants nor any ~~no~~ public officer shall, directly or through any other person, carry out any covert surveillance.

(2) Subsection (1) does not apply to any covert surveillance carried out pursuant to a prescribed authorization.

PART 3 PRESCRIBED AUTHORIZATIONS, ETC.

Division 1—Relevant Authorities

6. Panel judges

(1) ~~The Chief Executive shall, on the recommendation of the~~ Chief Justice shall; appoint 3 to 6 eligible judges to be panel judges for the purposes of this Ordinance.

(2) A panel judge shall be appointed for a period of 3 years, and may from time to time be reappointed.

(3A) ~~The Chief Executive may, on the recommendation of the Chief Justice, revoke the appointment of a panel judge for good cause. In performing any of his functions under the Ordinance, a panel judge has the same powers, protection and immunities as a judge of the Court of First Instance, but is not regarded as a court or member of a court.~~

(3B) For the purpose of performing any of his functions under this Ordinance, a panel judge may administer oaths and take affidavits.

(3C) Panel judges shall not sit as ordinary judges during their appointment as panel judges.

(4) Schedule 2 applies to and in relation to the procedures of, and other matters relating to, a panel judge.

(5) In this section, “eligible judge” (合資格法官) means a judge of the Court of First Instance.

7. Authorizing officers

The head of a department may designate any officer not below a rank equivalent to that of senior superintendent of police to be an authorizing

officer for the purposes of this Ordinance.

Division 2—Judicial Judge’s Authorizations

Issue of judicial judge’s authorizations

8. Application for judicial judge’s authorization for interception or Type 1 surveillance

(1) An officer of a department may apply to a panel judge for the issue of an judicial authorization for any interception or Type 1

surveillance to be carried out by or on behalf of any of the officers of the department.

(1A) An application under (1) shall be made ex parte in writing and supported by an affidavit of the applicant.

(1B) The panel judge may order a hearing to be held and any informant questioned or determine the application without a hearing. Any hearing of the application shall be held in private.

(1C) Regardless of whether a hearing is held the panel judge shall give his determination and his reasons for determination in writing.

(1D) Documents and records compiled by or made available to the panel judge shall be maintained as provided in Schedule 2.

(2) The application is an affidavit in support of an application under (1) shall—

(a) to be made in writing; and

(b) to be supported by an affidavit of the applicant which is to comply with the requirements specified in Part 1 or Part 2 of Schedule 3 as the case may be.—

(i) in the case of a judicial authorization for interception, Part 1 of Schedule 3; or

(ii) in the case of a judicial authorization for Type 1 surveillance, Part 2 of Schedule 3.

(3) An application may not be made under subsection (1) unless the making of the application has been approved by a directorate officer of the department concerned.

9. Determination of application for judicial authorization

(1) Upon considering an application for the issue of an judicial authorization made under section 8, the panel judge may, subject to subsection (2)—

(a) issue the judicial authorization sought under the application, with or without variations; or

(b) refuse to issue the judicial authorization.

(2) The panel judge shall not issue the ~~judicial~~ authorization unless he is satisfied that the conditions for its issue under section 3 have been met.

(3) The panel judge shall deliver his determination under subsection (1) ~~by—~~

~~(a) in the case of subsection (1)(a), issuing the judicial authorization, in writing; or~~

~~(b) in the case of subsection (1)(b), giving the reason for the refusal in writing.~~

10. Duration of ~~judicial judge' s~~ authorization

An ~~judicial~~ authorization—

(a) takes effect at the time specified by the panel judge when issuing the ~~judicial~~ authorization, which in any case is not to be earlier than the time when it is issued; and

(b) subject to any renewal under this Division, ceases to have effect upon the expiration of the period specified by the panel judge when issuing the ~~judicial~~ authorization, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Renewal of ~~judicial judge' s~~ authorizations

11. Application for renewal of ~~judicial judge' s~~ authorization

(1) At any time before a ~~judicial judge' s~~ authorization ceases to have effect, an officer of the department concerned may apply ~~to a panel judge~~ for the renewal of the ~~judicial~~ authorization.

(2) ~~The application is—~~ An application under (1) shall be made ex parte in writing and supported by—

~~(a) to be made in writing; and~~

~~(b) to be supported by—~~

- (i) a copy of the ~~judicial-judge'~~ s authorization sought to be renewed;
- (ii) a copy of ~~any~~ every affidavit provided under this Part for the purposes of any application for the issue or renewal of the ~~judicial~~ authorization, or for the purposes of any application made further to an ~~oral~~ application for confirmation of ~~the~~ judicial an emergency authorization or its ~~previous~~ renewal; and
- (iii) an affidavit of the applicant which is to comply with the requirements specified in Part 4 of Schedule 3.

(2A) The panel judge may order a hearing to be held and any informant to be questioned or determine the application without a hearing. Any hearing of the application shall be held in private.

(3) An application may not be made under subsection (1) unless the making of the application has been approved by a directorate officer of the department concerned.

12. Determination of application for renewal of ~~judicial-judge'~~ s authorization

(1) Upon considering an application for the renewal of a ~~judicial judge'~~ s authorization made under section 11, the panel judge may, subject to subsection (2)—

(a) grant the renewal sought under the application, with or without variations; or

(b) refuse to grant the renewal.

(2) The panel judge ~~shall not grant the renewal unless he is satisfied that the conditions for its grant under section 3 have been met.~~

(a) shall not grant the renewal unless he is satisfied that the conditions under section 3 are met; and

(b) shall take into account the total duration of the interception or covert surveillance as the case may be under authorization.

(3) The panel judge shall deliver his determination under subsection (1) by—

- (a) in the case of subsection (1)(a), issuing the renewed judicial authorization and reasons for the renewal in writing; or
- (b) in the case of subsection (1)(b), giving the reason for the refusal in writing.
- (4) A judicial authorization may be renewed more than once but in any event not more than a total of 2 years in duration under this Ordinance.

13. Duration of renewal of judicial authorization

A renewal of a judicial authorization—

- (a) takes effect at the time when the judicial authorization would have ceased to have effect but for the renewal; and
- (b) subject to any further renewal under this Division, ceases to have effect upon the expiration of the period specified by the panel judge when granting the renewal, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Division 3—Executive Authorizations

Issue of executive authorizations

14. Application for executive authorization for Type 2 surveillance

- (1) An officer of a department in charge of the investigation of the subject of interception or surveillance may apply to an authorizing officer of the department for the issue of an executive authorization for any Type 2 surveillance to be carried out by or on behalf of any of the officers of the department.
- (2) The application is—
 - (a) to be made in writing; and
 - (b) to be supported by a statement in writing made by the applicant which is to comply with the requirements specified in Part 3 of Schedule 3.

15. Determination of application for executive authorization

(1) Upon considering an application for the issue of an executive authorization made under section 14, the authorizing officer may, subject to subsection (2)—

(a) issue the executive authorization sought under the application, with or without variations; or

(b) refuse to issue the executive authorization.

(2) The authorizing officer shall not issue the executive authorization unless he is satisfied that the conditions for its issue under section 3 have been met.

(3) The authorizing officer shall deliver his determination under subsection (1) by—

(a) in the case of subsection (1)(a), issuing the executive authorization and giving reasons for the authorization in writing; or

(b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

16. Duration of executive authorization

An executive authorization—

(a) takes effect at the time specified by the authorizing officer when issuing the executive authorization, which in any case is not to be earlier than the time when it is issued; and

(b) subject to any renewal under this Division, ceases to have effect upon the expiration of the period specified by the authorizing officer when issuing the executive authorization, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Renewal of executive authorizations

17. Application for renewal of executive authorization

(1) At any time before an executive authorization ceases to have effect, an officer of the department concerned may apply to an authorizing officer of

the department for the renewal of the executive authorization.

(2) The application is—

- (a) to be made in writing; and
- (b) to be supported by—
 - (i) a copy of the executive authorization sought to be renewed;
 - (ii) a copy of any statement provided under this Part for the purposes of any application for the issue or renewal of the executive authorization, or for the purposes of any application made further to an oral application for confirmation of the executive authorization or its previous renewal; and
 - (iii) a statement in writing made by the applicant which is to comply with the requirements specified in Part 4 of Schedule 3.

18. Determination of application for renewal of executive authorization

- (1) Upon considering an application for the renewal of an executive authorization made under section 17, the authorizing officer may, subject to subsection (2)—
 - (a) grant the renewal sought under the application, with or without variations; or
 - (b) refuse to grant the renewal.
- (2) The authorizing officer ~~shall not grant the renewal unless he is satisfied that the conditions for its grant under section 3 have been met.~~
 - (a) shall not grant the renewal unless he is satisfied that the conditions for its grant under section 3 have been met; and
 - (b) shall take into account the total duration of the surveillance under the authorization.
- (3) The authorizing officer shall deliver his determination under subsection (1) by—
 - (a) in the case of subsection (1)(a), issuing the renewed executive authorization and giving his reasons for the renewal in writing; or
 - (b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

(4) An executive authorization may be renewed more than once but in any event not more than a total of 2 years in duration under this Ordinance.

19. Duration of renewal of executive authorization

A renewal of an executive authorization—

- (a) takes effect at the time when the executive authorization would have ceased to have effect but for the renewal; and
- (b) subject to any further renewal under this Division, ceases to have effect upon the expiration of the period specified by the authorizing officer when granting the renewal, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Division 4—Emergency Authorizations

Issue of emergency authorizations

20. Application for emergency authorization for interception or Type 1 surveillance in case of emergency

- (1) An officer of a department may apply to the head of the department for the issue of an emergency authorization for any interception or Type 1 surveillance to be carried out by or on behalf of any of the officers of the department, ~~if he considers that~~where—
 - (a) there is immediate need for the interception or Type 1 surveillance to be carried out by reason of an imminent risk of—
 - (i) death or serious bodily harm of any person;
 - (ii) substantial damage to property; or
 - (iii) serious threat to public security; ~~or~~
 - ~~(iv) loss of vital evidence;~~ and
 - (b) having regard to all the circumstances of the case, it is not reasonably practicable to apply for the issue of a ~~judicial~~judge's authorization for the interception or Type 1 surveillance.

~~(2) The application is~~ Subject to (3) an application for emergency authorization shall be—

(a) ~~to be~~ made in writing; and

(b) ~~to be~~ supported by a statement in writing made by the applicant which is to—

(i) set out the reason for making the application; and

(ii) comply with—

~~(A) in the case of an emergency authorization for interception,~~
the requirements specified in Part 1 or Part 2 of Schedule 3,
as the case may be which are to apply to the statement as they
apply to an affidavit referred to in section 8(2)(b); ~~or~~

~~(B) in the case of an emergency authorization for Type 1
surveillance, the requirements specified in Part 2 of Schedule
3 which are to apply to the statement as they apply to an
affidavit referred to in section 8(2)(b).~~

(3) An application for emergency authorization under (1) may be made orally in person if, having regard to all circumstances of the case, it is not reasonably practicable to make an application in writing.

(4) Where an oral application is made, the applicant shall make an oral statement providing the required information specified in Part 2 or Part 2 of Schedule 3 as the case may be.

21. Determination of application for emergency authorization

(1) Upon considering an application for the issue of an emergency authorization made under section 20, the head of the department concerned may, subject to subsection (2)—

(a) issue the emergency authorization sought under the application, with or without variations; or

(b) refuse to issue the emergency authorization.

(2) The head of the department shall not issue the emergency authorization unless he is satisfied—

(a) that section 20(1)(a) and (b) applies;

(aa) that, where an oral application is made, section 20(3) applies; and

(b) that the conditions for the issue of the emergency authorization under section 3 have been met.

(3) The head of the department shall deliver his determination under subsection (1) by—

(a) in the case of subsection (1)(a), issuing the emergency authorization and giving his reasons for the authorization in writing; or

(b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

22. Duration of emergency authorization

(1) An emergency authorization—

(a) takes effect at the time specified by the head of the department concerned when issuing the emergency authorization, which in any case is not to be earlier than the time when it is issued; and

(b) ceases to have effect upon the expiration of the period specified by the head of the department when issuing the emergency authorization, which in any case is not to be longer than the period of 48 hours beginning with the time ~~when it takes effect~~ of the issuance of the authorization.

(2) Without prejudice to any application under section 8 for the issue of any ~~judicial judge'~~ s authorization for the interception or Type 1 surveillance concerned, an emergency authorization may not be renewed under this Ordinance.

Application for confirmation of emergency authorizations

23. Application for confirmation of emergency authorization

(1) Where ~~any~~ an authorization for interception or Type 1 surveillance is issued as a result of an emergency application ~~carried out pursuant to an emergency authorization~~, the

head of the department concerned shall cause an officer of the department to apply to a panel judge for confirmation of the emergency authorization, as soon as reasonably practicable ~~after~~, and in any event within ~~the period of~~ 48 hours ~~beginning with, the time when of~~ the issuance of the emergency authorization ~~takes effect.~~

(2) The application for confirmation shall be—

(a) ~~to be~~ made in writing; and

(b) ~~to be~~ supported by—

(i) a copy of the emergency authorization; and

(ii) an affidavit of the applicant which verifies ~~is to verify~~ the contents of the statement provided under section 20(2)(b) or 20(4) as applicable for the purposes of the application for ~~the issue of the~~ emergency authorization.

(3) ~~If Where~~ no application for confirmation of the emergency authorization is made within the period of 48 hours referred to in subsection (1), ~~the head of the department concerned shall —~~ (a) the emergency authorization shall be void and of no effect from the time issued;

(b) without prejudice to section 52, the head of the department concerned shall submit a report to the Commissioner with the details of the case; and

(c) (a) cause the immediate destruction of any information obtained by carrying out the interception or Type 1 surveillance concerned shall be preserved for sole the propose of the Commissioner' s review or examination under Part4, to the extent that it could not have been obtained without carrying out the interception or Type 1 surveillance; and

~~(b) without prejudice to section 52, submit to the Commissioner a report with details of the case.~~

24. Determination of application for confirmation of emergency authorization

(1) Upon considering an application for confirmation of an emergency authorization as provided for in section 23(1), the panel judge may, subject to subsection (2)—

- (a) confirm the emergency authorization; or
- (b) refuse to confirm the emergency authorization.

(2) The panel judge shall not confirm the emergency authorization unless he is satisfied that section 21(2)(a) and (b) havees been complied with in the issue of the emergency authorization.

(3) Where the panel judge refuses to confirm the emergency authorization under subsection (1)(b), he may make one or more of the following orders—

~~(a) in any case where the emergency authorization still has effect at the time of the determination, an order that the emergency authorization is, notwithstanding any other provision of this Ordinance—~~

- ~~(i) an order revoking the emergency authorization;~~
- ~~(ii) an order that the emergency authorization have effect subject to the variation specified by the panel judge;~~
- ~~(iii) an order that the revocation takes effect upon the making of the determination;~~
- ~~(iv) an order that the emergency authorization is to be given no effect from the time of its issuance;~~
- ~~(v) an order that the head of the department preserves any information obtained under the emergency authorization for the sole purpose of a report to and investigation by the Commissioner, to be revoked upon the making of the determination; or~~

~~(ii) only to have effect subject to the variations specified by him, from the time of the determination;~~

~~(b) in any case whether or not the emergency authorization still has effect at the time of the determination, an order that the head of the department concerned shall cause the immediate destruction of any information obtained by~~

- ~~carrying out the interception or Type 1 surveillance concerned, to the extent—~~
~~(i) subject to subparagraph (ii), that it could not have been obtained without carrying out the interception or Type 1 surveillance; or~~
~~(ii) where paragraph (a)(ii) applies, that is specified in the order.~~
~~(4) Where the emergency authorization is revoked under subsection (3)(a)(i), the emergency authorization is, notwithstanding section 22(1)(b), to cease to have effect from the time of the revocation.~~
- (5) The panel judge shall deliver his determination under subsection (1) by—
- (a) in the case of subsection (1)(a), endorsing his confirmation on the emergency authorization and giving his reasons for the confirmation in writing; or
 - (b) in the case of subsection (1)(b), giving the reason for the refusal and making any order under subsection (3) in writing.

Division 5—Special Provisions for Oral Applications

Oral applications

25. Oral application and its effect

- ~~(1) Notwithstanding the relevant written application provision, an application for the issue or renewal of a prescribed authorization under this Ordinance may be made orally, if the applicant considers that, having regard to all the circumstances of the case, it is not reasonably practicable to make the application in accordance with the relevant written application provision.~~
- ~~(2) Notwithstanding the relevant determination provision and without prejudice to the relevant conditions provision, where an oral application is made, the relevant authority shall not issue or grant the prescribed authorization or renewal sought under the application unless he is satisfied that, having regard to all the~~

~~circumstances of the case, it is not reasonably practicable to make the application in accordance with the relevant written application provision.~~

~~(3) Notwithstanding the relevant document provision, where an oral application is made, the information required to be provided for the purposes of the application under the relevant document provision may be provided orally (and accordingly any requirement as to the making of any affidavit or statement does not apply).~~

~~(4) Notwithstanding the relevant written determination provision, where an oral application is made, the relevant authority may deliver the determination required to be delivered in respect of the application under the relevant determination provision by—~~

~~(a) issuing the prescribed authorization or the renewed prescribed authorization orally; or~~

~~(b) where he refuses to issue or grant the prescribed authorization or renewal sought under the application, giving the reason for the refusal orally.~~

~~(5) Except as otherwise provided in this Division, any oral application and any prescribed authorization or renewal issued or granted as a result of that application are for all purposes regarded as having the same effect respectively as an application made in writing and a prescribed authorization or renewal issued or granted as a result of that application, and the provisions of this Ordinance are, subject to necessary modifications, to apply accordingly.~~

~~(6) In this section—~~

~~“relevant conditions provision” (有關條件條文) means section 9(2), 12(2), 15(2),~~

~~18(2) or 21(2) (as may be applicable);~~

~~“relevant determination provision” (有關決定條文) means section 9(1), 12(1),~~

~~15(1), 18(1) or 21(1) (as may be applicable);~~

~~“relevant document provision” (有關文件條文) means section 8(2)(b), 11(2)(b),~~

~~14(2)(b), 17(2)(b) or 20(2)(b) (as may be applicable);~~
~~“relevant written application provision” (有關書面申請條文)~~
~~means section 8(2)(a), 11(2)(a), 14(2)(a), 17(2)(a) or 20(2)(a) (as~~
~~may be applicable);~~
~~“relevant written determination provision” (有關書面決定條文)~~
~~means section 9(3), 12(3), 15(3), 18(3) or 21(3) (as may be~~
~~applicable).~~

~~Application for confirmation of prescribed authorizations or~~
~~renewals issued or granted upon oral applications~~
 26. ~~Application for confirmation of prescribed~~
~~authorization or renewal issued or granted upon oral application~~
 (1) ~~Where, as a result of an oral application, the prescribed~~
~~authorization or renewal sought under the application has been~~
~~issued or granted, the head of the department concerned shall cause~~
~~an officer of the department to apply to the relevant authority for~~
~~confirmation of the prescribed authorization or~~
~~renewal, as soon as reasonably practicable after, and in any event~~
~~within the period of 48 hours beginning with, the time when the~~
~~prescribed authorization~~
~~or renewal takes effect.~~
 (2) ~~The application is—~~
 (a) ~~to be made in writing; and~~
 (b) ~~to be supported by—~~
 (i) ~~a record in writing containing all the information that~~
 ~~would have been provided to the relevant authority in writing~~
 ~~under the relevant written application provision had the oral~~
 ~~application been made in writing;~~
 (ii) ~~where section 25(3) applies in relation to the oral~~
 ~~application—~~
 (A) ~~where the relevant authority is a panel judge, an~~
 ~~affidavit of the applicant which is to verify all the~~
 ~~information provided pursuant to that section for the~~
 ~~purposes of the oral application; or~~

~~(B) where the relevant authority is not a panel judge, a statement in writing made by the applicant setting out all the information provided pursuant to that section for the purposes of the oral application; and~~

~~(iii) where section 25(4) applies in relation to the oral application, a record in writing setting out the determination delivered pursuant to that section in respect of the oral application.~~

~~(3) If no application for confirmation of the prescribed authorization or renewal is made within the period of 48 hours referred to in subsection (1), then—~~

~~(a) in any case where the prescribed authorization or renewal still has effect upon the expiration of the period, the prescribed authorization or renewal is, notwithstanding any other provision of this Ordinance, to be regarded as revoked upon the expiration of the period; and~~

~~(b) in any case whether or not the prescribed authorization or renewal still has effect upon the expiration of the period, the head of the department concerned shall—~~

~~(i) cause the immediate destruction of any information obtained by carrying out the interception or covert surveillance concerned, to the extent that it could not have been obtained without carrying out the interception or covert surveillance; and~~

~~(ii) without prejudice to section 52, submit to the Commissioner a report with details of the case.~~

~~(4) Where the prescribed authorization or renewal is regarded as revoked under subsection (3)(a), the prescribed authorization or renewal is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.~~

~~(5) In this section—~~

~~“relevant duration provision” (有關時限條文) means section 10(b), 13(b), 16(b) or 19(b) (as may be applicable);~~

~~“relevant written application provision” (有關書面申請條文)~~
~~means section 8(2)(a), 11(2)(a), 14(2)(a), 17(2)(a) or 20(2)(a) (as~~
~~may be applicable).~~

~~27. Determination of application for confirmation of
prescribed authorization or renewal issued or granted upon oral
application~~

- ~~(1) Upon considering an application for confirmation of a
prescribed authorization or renewal as provided for in section
26(1), the relevant authority may, subject to subsection (2)—~~
~~(a) confirm the prescribed authorization or renewal; or~~
~~(b) refuse to confirm the prescribed authorization or renewal.~~
~~(2) The relevant authority shall not confirm the prescribed
authorization or renewal unless he is satisfied that the relevant
conditions provision has been complied with in the issue or grant
of the prescribed authorization or renewal.~~
~~(3) Where the relevant authority refuses to confirm the prescribed
authorization or renewal under subsection (1)(b), he may make one
or more of the following orders—~~
~~(a) in any case where the prescribed authorization or renewal still
has effect at the time of the determination, an order that the
prescribed authorization or renewal is, notwithstanding any other
provision of this Ordinance—~~
~~(i) to be revoked upon the making of the determination; or~~
~~(ii) only to have effect subject to the variations specified by
him, from the time of the determination;~~
~~(b) in any case whether or not the prescribed authorization or
renewal still has effect at the time of the determination, an order
that the head of the department concerned shall cause the
immediate destruction of any information obtained by carrying
out the interception or covert surveillance concerned, to the
extent—~~
~~(i) subject to subparagraph (ii), that it could not have been
obtained without carrying out the interception or covert
surveillance; or~~

- (ii) ~~where paragraph (a)(ii) applies, that is specified in the order.~~
- (4) ~~Where the prescribed authorization or renewal is revoked under subsection (3)(a)(i), the prescribed authorization or renewal is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.~~
- (5) ~~The relevant authority shall deliver his determination under subsection (1) by—~~
 - (a) ~~in the case of subsection (1)(a), issuing the prescribed authorization or the renewed prescribed authorization (being the prescribed authorization confirmed under that subsection or being in terms of the renewal confirmed under that subsection (as the case may be)) in writing; or~~
 - (b) ~~in the case of subsection (1)(b), giving the reason for the refusal and making any order under subsection (3) in writing.~~
- (6) ~~In this section—~~
 - ~~“relevant conditions provision” (有關條件條文) means section 9(2), 12(2), 15(2), 18(2) or 21(2)(b) (as may be applicable);~~
 - ~~“relevant duration provision” (有關時限條文) means section 10(b), 13(b), 16(b), 19(b) or 22(1)(b) (as may be applicable).~~

28. ~~Special case of emergency authorization issued as a result of oral application~~

- (1) ~~Where an emergency authorization is issued as a result of an oral application, sections 26 and 27 do not apply if—~~
 - (a) ~~an application for confirmation of the emergency authorization as provided for in section 23(1) has been made to a panel judge within the period of 48 hours referred to in that section; and~~
 - (b) ~~the application is supported by—~~
 - (i) ~~a record referred to in section 26(2)(b)(i);~~
 - (ii) ~~an affidavit of the applicant which is to verify the contents of the statement provided under section 20(2)(b) for the purposes of the application for the issue of the emergency~~

~~authorization or, where section 25(3) applies in relation to the oral application, all the information provided pursuant to section 25(3) for the purposes of the oral application; and (iii) a copy of the emergency authorization or, where section 25(4) applies in relation to the oral application, a record in writing setting out the determination delivered pursuant to that section in respect of the oral application.~~

~~(2) Notwithstanding section 23(2)(b), the application described in subsection (1)(a) and (b) is for all purposes regarded as an application duly made for confirmation of the emergency authorization as provided for in section 23(1), and the provisions of this Ordinance are to apply accordingly (subject to section 24(5)(a) being read as requiring the panel judge to deliver his determination under section 24(1) by issuing the emergency authorization (being the emergency authorization confirmed under section 24(1)(a)) in writing).~~

Division 6—General Provisions for Prescribed Authorizations

Matters authorized, required or provided for
by prescribed authorizations

29. What a prescribed authorization may authorize or require under or by virtue of its terms, etc.

(1A) A prescribed authorization for interception must specify the person or persons whose communications are to be the subject of interception and no authorization for interception shall be construed as authorizing the interception of any communication to or from any person other than the person or persons so specified.

(1AA) A prescribed authorization for covert surveillance must specify the person or persons who is to be the subject of covert surveillance and no authorization for covert surveillance shall be construed as authorizing the surveillance of any person other than the person or persons so specified.

(1) Subject to subsection (1A), a A prescribed authorization for interception may—

(a) in the case of a postal interception, contain terms that authorize one or both of the following—

- (i) the interception of communications made to or from any premises or address specified in the prescribed authorization;
- (ii) the interception of communications made to or by any person specified in the prescribed authorization (whether by name or by description); or

(b) in the case of a telecommunications interception, contain terms that authorize ~~one or both of the following—~~

- ~~(i) the interception of communications made to or from any telecommunications service specified in the prescribed authorization;~~
- ~~(ii) the interception of communications made to or from any telecommunications service that any person specified in the prescribed authorization (whether by name or by description) is using, or is likely to use.~~

(2) Subject to subsection (1AA), a A prescribed authorization for covert surveillance may contain terms that authorize one or more of the following—

- (a) the use of any surveillance devices in or on any premises specified in the prescribed authorization as the place for installation of the surveillance device;
- (b) the use of any surveillance devices in or on any object or class of objects specified in the prescribed authorization;
- (c) the use of any surveillance devices in respect of the conversations, activities or location of any person specified in the prescribed authorization (whether by name or by description).

(3) A prescribed authorization, other than an executive authorization, may contain terms that authorize the doing of anything lawful and reasonably necessary to conceal any conduct authorized or required to be carried out under the prescribed authorization.

(4) A prescribed authorization, other than an executive authorization, may, if it is necessary for the execution of the prescribed authorization, contain terms that authorize the interference with any property (whether or not of any person who is the subject of the interception or covert surveillance concerned) provided that the nature of the interference so authorized must be specified in the authorization.

(5) A prescribed authorization, other than an executive authorization, may contain terms that require any person specified in the prescribed authorization (whether by name or by description), on being shown a copy of the prescribed authorization, to provide to any of the officers of the department concerned such assistance for the execution of the prescribed authorization as is specified in the prescribed authorization.

(6) A prescribed authorization for interception also authorizes—
 (a) the installation, use and maintenance of any devices required to be used in order to intercept any of the communications authorized to be intercepted under the prescribed authorization provided that if the device is to be installed in or used from any private property, the address and if ascertainable, the owner, tenant and occupier of such property must be specified in the authorization ;

(b) subject to (a) above, the entry, by force if necessary, onto any premises in order to carry out any conduct authorized or required to be carried out under the prescribed authorization;

(c) the interception of any communication which it is necessary to intercept in order to intercept any of the communications authorized to be intercepted under the prescribed authorization;
 and

(d) where subsection (1)(a)(ii) or (b)(ii) is applicable, the provision to any person, for the execution of the prescribed authorization, of particulars of the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying—

- (i) in the case of subsection (1)(a)(ii), the communications made to or by the person specified in the prescribed authorization; or
 - (ii) in the case of subsection (1)(b)(ii), the communications made to or from any telecommunications service that the person specified in the prescribed authorization is using, or is likely to use.
- (7) A prescribed authorization for covert surveillance also authorizes—
- (a) where subsection (2)(a) is applicable—
 - (i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization in or on the premises specified in the prescribed authorization provided that if the device is to be installed in or used from any private property, the address and if ascertainable, the owner, tenant and occupier of such property must be specified in the authorization ; and
 - (ii) subject to (i) above the entry, by force if necessary, onto the premises, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization;
 - (b) where subsection (2)(b) is applicable—
 - (i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization in or on the object, or an object of the class, specified in the prescribed authorization; and
 - (ii) the entry, by force if necessary, onto any premises where the object, or an object of the class, is reasonably believed to be or likely to be, and onto any other premises adjoining or providing access to the premises in order to carry out any conduct authorized or required to be carried out under the prescribed authorization provided that if the device is to be installed in or used from any private property, the address

- and if ascertainable, the owner, tenant and occupier of such property must be specified in the authorization; and
- (c) where subsection (2)(c) is applicable—
- (i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization, in or on any premises where the person specified in the prescribed authorization is reasonably believed to be or likely to be provided that if the device is to be installed in or used from any private property, the address and if ascertainable, the owner, tenant and occupier of such property must be specified in the authorization ; and
 - (ii) subject to (i) above, the entry, by force if necessary, onto the premises, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization.

30. What a prescribed authorization further authorizes

~~A~~ Subject to section 29, a prescribed authorization further authorizes the undertaking of any lawful conduct which it is necessary to undertake in order to carry out what is authorized or required to be carried out under the prescribed authorization and, without limiting the generality of the foregoing, such conduct includes—

- (a) the retrieval of any of the devices authorized to be used under the prescribed authorization;
- (b) the installation, use, maintenance and retrieval of any enhancement equipment for the devices;
- (c) the temporary removal of any conveyance or object from any premises for the installation, maintenance or retrieval of the devices or enhancement equipment and the return of the conveyance or object to the premises;
- (d) the breaking open of anything for the installation, maintenance or retrieval of the devices or enhancement equipment;

- (e) the connection of the devices or enhancement equipment to any source of electricity and the use of electricity from that source to operate the devices or enhancement equipment;
- (f) the connection of the devices or enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the devices or enhancement equipment; and
- (g) the provision of assistance for the execution of the prescribed authorization.

30A. What a prescribed authorization may not authorize

(1) Notwithstanding anything in this Ordinance, subject to subsection (2)—

- a. no prescribed authorization may contain terms that authorize the interception of communications by reference to—
 - i. in the case of a postal interception, an office or other relevant premises, or a residence of a lawyer; or
 - ii. in the case of a telecommunications interception, any telecommunications service used at an office or other relevant premises, or a residence, of a lawyer, or any telecommunications service known or reasonably expected to be known by the applicant to be ordinarily used by a lawyer for the purpose of providing legal advice to clients; and
- b. no prescribed authorization may contain terms that authorize any covert surveillance to be carried out in respect of oral or written communications taking place at an office or other relevant premises, or a residence, of a lawyer; and
- c. no prescribed authorization may contain terms that authorize any covert surveillance to be carried out in respect of oral or written communications taking place in any place provided for legal visits by lawyers visiting

- prisons or other places of detention or in any place where a lawyer is visiting any other person in detention
- (2) a prescribed authorization may contain terms that authorize
- i. the interception of a communication service used by a lawyer other than a service referred to in (1)(a)(ii); or
 - ii. covert surveillance to be carried out in respect of oral or written communications taking place at the residence of a lawyer
- if the relevant authority is satisfied that there is credible evidence to justify a reasonable belief that the lawyer concerned is a party to any activity which constitutes or would constitute a serious crime or threat to public security and the communications concerned is for the furtherance of that criminal purpose, or that threat to public security.
- (3) For the avoidance of doubt, a prescribed authorization does not authorize any device to be implanted in, or administered to, a person without the consent of the person.
- (4) In this section—
- “lawyer” means a barrister, solicitor or foreign lawyer as defined in section 2(1) of the Legal Practitioners Ordinance (Cap. 159) who practices as such, or any person holding an appointment under section 3(1) of the Legal Aid Ordinance (Cap. 91);
- “other relevant premises” in relation to a lawyer, means any premises, other than an office of the lawyer, that are known or reasonably expected to be known by the applicant to be ordinarily used by the lawyer and by other lawyers for the purpose of providing legal advice to clients.

31. Prescribed authorization may be issued or renewed

subject to conditions

A prescribed authorization may be issued or renewed subject to any conditions specified in it that apply to the prescribed authorization itself or to any further authorization or requirement under it (whether granted or imposed under its terms or any provision of this Ordinance).

Device retrieval warrants after prescribed authorizations having ceased to have effect

32. Application for device retrieval warrant

(1) Where a prescribed authorization has in any way ceased to have effect under this Ordinance, an officer of the department concerned may apply, *ex parte*, to a panel judge for the issue of a device retrieval warrant authorizing the retrieval of any of the devices authorized to be used under the prescribed authorization if such devices—

(a) have been installed in or on any premises or object, pursuant to the prescribed authorization; and

(b) are still in or on such premises or object, or are in or on any other premises or object.

(2) The application is—

(a) to be made in writing; and

(b) to be supported by—

(i) a copy of the prescribed authorization; and

(ii) an affidavit of the applicant which is to comply with the requirements specified in Schedule 4.

33. Determination of application for device retrieval warrant

(1) Upon considering an application for the issue of a device retrieval warrant made under section 32, the panel judge may, subject to subsection (2)—

(a) issue the device retrieval warrant sought under the application, with or without variations; or

(b) refuse to issue the device retrieval warrant.

(2) The panel judge shall not issue the device retrieval warrant unless he is satisfied that section 32(1)(a) and (b) applies to the devices concerned.

(3) The panel judge shall deliver his determination under subsection (1) by—

(a) in the case of subsection (1)(a), issuing the device retrieval warrant and giving reasons for the issuance of the warrant in writing; or

(b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

34. Duration of device retrieval warrant

A device retrieval warrant—

(a) takes effect at the time specified by the panel judge when issuing the warrant, which in any case is not to be earlier than the time when it is issued; and

(b) ceases to have effect upon the expiration of the period specified by the panel judge when issuing the warrant, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

35. What a device retrieval warrant may authorize under or by virtue of its terms, etc.

(1) A device retrieval warrant may authorize the retrieval of any devices specified in the warrant.

(2) A device retrieval warrant may contain terms that authorize the doing of anything reasonably necessary to conceal any conduct authorized to be carried out under the warrant.

(3) A device retrieval warrant may, if it is necessary for the execution of the warrant, contain terms that authorize the interference with any property (whether or not of any person who is the subject of the interception or covert surveillance concerned).

36. What a device retrieval warrant further authorizes

(1) A device retrieval warrant further authorizes the undertaking of any conduct which it is necessary to undertake in order to carry out what is authorized to be carried out under the warrant and, without limiting the generality of the foregoing, such conduct includes—

- (a) the retrieval of any enhancement equipment for the devices authorized to be retrieved under the warrant;
- (b) the entry, by force if necessary, onto any premises where the devices or enhancement equipment is reasonably believed to be or likely to be, and onto any other premises adjoining or providing access to the premises, in order to retrieve the devices or enhancement equipment;
- (c) the temporary removal of any conveyance or object from any premises for the retrieval of the devices or enhancement equipment and the return of the conveyance or object to the premises;
- (d) the breaking open of anything for the retrieval of the devices or enhancement equipment; and
- (e) the provision of assistance for the execution of the warrant.

(2) A device retrieval warrant which authorizes the retrieval of any tracking devices also authorizes the use of the tracking devices and any enhancement equipment for the tracking devices solely for the purposes of the location and retrieval of the tracking devices or enhancement equipment.

37. Device retrieval warrant may be issued subject to conditions
A device retrieval warrant may be issued subject to any conditions specified in it that apply to the warrant itself or to any further authorization under it (whether granted under its terms or any provision of this Ordinance).

PART 4

THE COMMISSIONER

Division 1—The Commissioner and his Functions

38. The Commissioner

(1) There is hereby established an office by the name of the Commissioner on Interception of Communications and Surveillance.

- (2) The Chief Executive shall, on the recommendation of the Chief Justice, appoint an eligible ~~judge~~ person to be the Commissioner.
- (3) The Commissioner shall be appointed for a period of 3 years, and may from time to time be reappointed.
- (4) The Commissioner shall be entitled to such remuneration and allowances as are determined by the Chief Executive.
- (5) The Chief Executive may, ~~on the recommendation of the Chief Justice,~~ revoke the appointment of the Commissioner for good cause provided that the reason for such revocation must be given in writing and shall be reviewable by a court of law.
- (6) In this section, “eligible ~~judge~~ person” (合資格法官) means—
- ~~(a) a Justice of Appeal of the Court of Appeal;~~
 - ~~(b) a judge of the Court of First Instance;~~
 - ~~(c) (a) a former permanent judge of the Court of Final Appeal;~~
 - ~~(d) (b) a former Justice of Appeal of the Court of Appeal; or~~
 - ~~(e) (c) a former judge of the Court of First Instance.~~

39. Functions of Commissioner

The functions of the Commissioner are—

- (a) to oversee the compliance by departments and their officers with the relevant requirements; and
- (b) without limiting the generality of paragraph (a), to—
 - (i) conduct reviews under Division 2;
 - (ii) carry out examinations under Division 3;
 - (iii) submit reports to the Chief Executive and make recommendations to the Secretary for Security and heads of departments under Division 4;
 - (iv) investigate complaints made by any person in relation to any interception or surveillance carried out whether with or without authorization
 - ~~(iv) (v)~~ perform any further functions prescribed by regulation made under section 62 for the purposes of this subparagraph; and

~~(v)~~ (vi) perform such other functions as are imposed or conferred on him under this Ordinance or any other enactment.

Division 2—Reviews by Commissioner

40. Reviews on compliance with relevant requirements

(1) The Commissioner shall conduct such reviews as he considers necessary on compliance by departments and their officers with the relevant requirements.

(1A) Without limiting the generality of subsection (1), the Commissioner shall conduct reviews on cases in respect of which a report has been submitted to him under section 23(3)(b), 24(3)(b)(v) or 52.

(2) Upon the conduct of any review under subsection (1), the Commissioner shall record in writing—

(a) details, as identified in the review, of any case of failure by any department or any of its officers to comply with any relevant requirement; and

(b) any other finding he has made in the review.

(3) The Commissioner shall have a general power to require any department to investigate any person within that department where a panel judge or he determines that there is reasonable grounds to believe that the person concerned has contravened provisions of the Ordinance or has presented false information in obtaining an authorization and to require a report from such department on the outcome of any investigation and any disciplinary action taken.

(4) The Commissioner shall have a general power to conduct any investigation as he considers necessary into the conduct of any person apart from a panel judge and to refer any matter to the Director of Public Prosecutions upon conclusion of such investigation.

41. Notifications to departments concerned, etc.

(1) The Commissioner shall notify the head of any department concerned of his findings in a review under section 40(2).

- (2) On being notified of the findings of the Commissioner under subsection (1), the head of the department shall submit to the Commissioner a report with details of any measures taken by the department to address any issues identified in the findings, as soon as reasonably practicable after the notification or, where the Commissioner has specified any period for submission of the report when giving the notification, within that period.
- (3) Without prejudice to sections 47 and 48, the Commissioner may, whether before or after the head of the department has submitted a report to him under subsection (2), refer the findings and any other matters he thinks fit to the Chief Executive or the Secretary for Justice or both.

Division 3—Examinations by Commissioner

42. Application for examination

- (1) A person may apply to the Commissioner for an examination under this Division, if he believes—
- (a) that any communication transmitted to or by him has been intercepted by a department; or
 - (b) that he is the subject of any covert surveillance that has been carried out by a department.
- (2) The application is to be made in writing.

43. Examination by Commissioner

- (1) Where the Commissioner in the course of performing any of his functions under this Ordinance considers or suspects that there is any case in which any interception or covert surveillance has been carried out in contravention of this Ordinance, or receives an application under section 42, he shall, subject to section 44, carry out an examination to determine—
- (a) whether or not the interception or covert surveillance alleged has taken place; and

(b) if so, whether or not the alleged interception or covert surveillance was carried out under the authority of a prescribed authority issued or renewed in accordance with this Ordinance ~~a prescribed authorization should have been, but has not been, issued or renewed under this Ordinance in relation to the interception or covert surveillance alleged.~~

(2) If, on an examination, the Commissioner determines that a prescribed authorization ~~should have been, but has not been, issued or renewed under this~~ Ordinance in relation to the interception or covert surveillance alleged, he—

~~(a) shall give notice to the applicant stating that he has found the case in the applicant's favour; and~~

~~(b) may, if he thinks fit, make an order for the payment of compensation by the Government to the applicant.~~ was issued or renewed in contravention of this Ordinance or should not have been issued or renewed or the interception or covert surveillance alleged has been carried out without the authority of a prescribed authorization issued or renewed under this Ordinance, he shall give notice as soon as practicable to the subject of interception or surveillance or the applicant—

(a) stating he has found the case in the subject of interception or surveillance's or the applicant's favour with particulars of his findings; and

(b) inviting the subject of interception or surveillance or the applicant to confirm whether the latter wishes to seek an order for the payment of compensation under the application, and if so, to make written submissions to him for that purpose.

(2A) Upon receiving confirmation from the applicant that an order for the payment of compensation is sought, the Commissioner, upon taking into account any written submissions made to him for the purpose, may make any order for the payment of compensation by the Government to the applicant.

(2B) The compensation ordered to be paid under subsection (2A) may include compensation for injury of feelings.

(3) If, on an examination, the Commissioner makes a determination other than that referred to in subsection (2), he shall give notice as soon as practicable to the applicant stating that he has not found the case in the applicant's favour.

~~(4) The compensation ordered to be paid under subsection (2)(b) may include compensation for injury to feelings.~~

(5) Notwithstanding subsections (2), (2A), and (3), the Commissioner shall not give any notice or make any order under those subsections for so long as he considers that the giving of the notice or the making of the order (as the case may be) would be prejudicial to the prevention or detection of crime or the protection of public security.

44. Grounds for not carrying out examination, etc.

(1) Where, before or in the course of an examination, the Commissioner considers—

(a) that the application for the examination is received by the Commissioner more than 4-5 year after the day on which the interception or covert surveillance is alleged to have taken place or, where the interception or covert surveillance is alleged to have taken place on more than 1 day, the last occasion on which it is alleged to have taken place, and that it is not unfair for him not to carry out the examination;

(b) that the application is made anonymously;

(c) that the applicant cannot be identified or traced; or

(d) that, having regard to all the circumstances of the case, the application is frivolous or vexatious or is not made in good faith, the Commissioner may refuse to carry out the examination or, where the examination has been commenced, to proceed with the carrying out of the examination (including the making of any determination further to the examination).

~~(2) Where, before or in the course of an examination, the Commissioner is satisfied that any relevant criminal proceedings~~

~~are pending or are likely to be instituted, the Commissioner shall not carry out the examination or, where the examination has been commenced, proceed with the carrying out of the examination (including the making of any determination further to the examination)—~~

~~(a) in the case of any pending criminal proceedings, until they have been finally determined or finally disposed of; or~~

~~(b) in the case of any criminal proceedings which are likely to be instituted, until they have been finally determined or finally disposed of or, if applicable, until they are no longer likely to be instituted.~~

~~(3) For the purposes of subsection (2), criminal proceedings are, in relation to an examination, regarded as relevant if, but only if, the interception~~

~~or covert surveillance alleged in the application for the examination is or may be relevant to the determination of any question concerning any evidence which has been or may be adduced in those proceedings.~~

45. Further provisions relating to examinations

(1) For the purposes of an examination, the Commissioner shall—

(a) except as otherwise provided in this Ordinance, apply the principles applicable by a court on an application for judicial review except that the burden of proving the interception or covert surveillance alleged to have been lawfully carried out shall lie with the government; and

(b) subject to section 51(1), carry out the examination on the basis of written submissions made to him.

(2) Without prejudice to section 51(3), for the purposes of an examination, the applicant is not entitled to have access to any information, document or other matter compiled by, or made available to, the Commissioner in connection with the examination.

(3) Without prejudice to section 43(5), in giving notice to an applicant under section 43(2)(a) or (3), the Commissioner ~~shall not~~—

- (a) shall give reasons for his determination;
- (b) shall not give details of any interception or covert surveillance concerned; and
- (c) in the case of section 43(3), shall not indicate whether or not the interception or covert surveillance alleged has taken place.

46. Notifications to departments concerned, etc.

- (1) Where, on an examination, the Commissioner makes a determination under section 43(2), he shall notify the head of the department concerned of the determination.
- (2) On being notified of the determination under subsection (1), the head of the department shall submit to the Commissioner a report with details of
any measures taken by the department to address any issues arising from the determination, as soon as reasonably practicable after the notification or, where the Commissioner has specified any period for submission of the report when giving the notification, within that period.
- (3) Without prejudice to sections 47 and 48, the Commissioner may, whether before or after the head of the department has submitted a report to
him under subsection (2), refer the determination and any other matters he thinks fit to the Chief Executive or the Secretary for Justice or both.

46A. Notifications to relevant persons

- (1) If, in the course of performing any of his functions under this Ordinance, the Commissioner considers that there is any case in which any interception or covert surveillance has been wrongly carried out or carried out without the authority of a prescribed authorization issued or renewed under, or constituted a material contravention of, this Ordinance, subject to subsection (6), the Commissioner shall give notice to the relevant person –

- (a) stating that there has been such a case and indicating whether the case is one of interception or covert surveillance and the duration of the interception or covert surveillance; and
- (b) informing the relevant person of his right to apply to the Commissioner for an examination in respect of the interception or covert surveillance.

(2) Where the relevant person makes an application for an examination in respect of the interception or covert surveillance within 6 months after receipt of the notice or within such further period as the Commissioner may allow, the Commissioner shall, notwithstanding anything in section 44(1)(a) but subject to the other provisions of section 44, make a determination referred to in section 43(2), and the provisions of this Ordinance are to apply accordingly.

(3) Notwithstanding subsection (1), the Commissioner shall not give any notice under that subsection for so long as he considers that the giving of the notice would be prejudicial to the prevention or detection of crime or the protection of public security.

- (4) Without prejudice to subsection (3), the Commissioner shall give reasons for his findings or so much of his reasons as would not be prejudicial to the prevention or detection of crime or the protection of public security.

(5) For the purposes of this section, in considering whether any interception or covert surveillance has been carried out without the authority of a prescribed authorization issued or renewed under this Ordinance, the Commissioner shall apply the principles applicable by a court on an ex parte application.

(6) This section does not require the Commissioner to give any notice to a relevant person if –

- (a) the relevant person cannot, after the use of reasonable efforts, be identified or traced;

- (b) the Commissioner considers that the intrusiveness of the interception or covert surveillance concerned on the relevant person is negligible; or
- (c) in the case of interception, it is within the description of section 4(2)(b) or (c).

(7) In this section, “relevant person” (有關人士) means any person who is the subject of the interception or covert surveillance concerned or such person as being affected by interception or covert surveillance carried out.

Division 4—Reports and Recommendations by Commissioner

~~47. Annual reports to Chief Executive by Commissioner~~

~~(1) The Commissioner shall, for each report period, submit a report to the Chief Executive.~~

~~(2) A report for a report period is to set out, separately in relation to interception and covert surveillance—~~

~~(a) a list showing—~~

~~(i) the number of prescribed authorizations issued under this Ordinance during the report period, and the average duration of the prescribed authorizations;~~

~~(ii) the number of prescribed authorizations renewed under this Ordinance during the report period, and the average duration of the renewals;~~

~~(iii) the number of applications for the issue of prescribed authorizations made under this Ordinance that have been refused during the report period; and~~

~~(iv) the number of applications for the renewal of prescribed authorizations made under this Ordinance that have been refused during the report period;~~

~~(b) a list showing—~~

~~(i) the major categories of offences for the investigation of which prescribed authorizations have been issued or renewed under this Ordinance during the report period; and~~

- ~~(ii) the number of persons arrested during the report period as a result of or further to any interception or covert surveillance carried out pursuant to a prescribed authorization;~~
- ~~(c) a list showing—~~
 - ~~(i) the number of device retrieval warrants issued under this Ordinance during the report period, and the average duration of the warrants; and~~
 - ~~(ii) the number of applications for the issue of device retrieval warrants made under this Ordinance that have been refused during the report period;~~
- ~~(d) a list showing—~~
 - ~~(i) a summary of reviews conducted by the Commissioner under section 40 during the report period;~~
 - ~~(ii) the number and broad nature of any cases of irregularities identified in the reviews during the report period;~~
 - ~~(iii) the number of applications for examination that have been received by the Commissioner during the report period;~~
 - ~~(iv) a summary of the determinations of the Commissioner on examinations carried out during the report period; and~~
 - ~~(v) the broad nature of recommendations made by the Commissioner under sections 49 and 50 during the report period; and~~
 - ~~(e) an assessment on the overall compliance with the relevant requirements during the report period.~~
- ~~(3) The report is to be submitted within 6 months after the expiry of the report period.~~
- ~~(4) Subject to subsection (5), the Chief Executive shall cause a copy of the report to be laid on the table of the Legislative Council.~~
- ~~(5) If the Chief Executive considers that the publication of any matter in the report referred to in subsection (4) would be prejudicial to the prevention or detection of crime or the protection of public security, he may, after consultation with the Commissioner, exclude such matter from the copy of the report to be laid on the table of the Legislative Council under that subsection.~~

~~(6) In this section, “report period” (報告期間), in relation to a report required to be submitted under subsection (1), means—~~
~~(a) the period beginning on the commencement of this Ordinance and ending on 31 December in the same year; or~~
~~(b) any of the succeeding periods of 12 months ending on 31 December.~~

47. Annual reports to Chief Executive by Commissioner

(1) The Commissioner shall, for each report period, submit a report to the Chief Executive.

(2) A report for a report period is to set out, separately in relation to interception and covert surveillance –

(a) a list showing –

- (i) the respective numbers of judge’s authorizations, executive authorizations and emergency authorizations issued under this Ordinance during the report period, and the average duration of the respective prescribed authorizations;
- (ii) the respective numbers of judge’s authorizations and executive authorizations renewed under this Ordinance during the report period, and the average duration of the respective renewals;
- (iii) the respective numbers of judge’s authorizations, executive authorizations and emergency authorizations issued as a result of an oral application under this Ordinance during the report period, and the average duration of the respective prescribed authorizations;

- (iv) the respective numbers of judge's authorizations and executive authorizations renewed as a result of an oral application under this Ordinance during the report period, and the average duration of the respective renewals;
- (v) the respective numbers of judge's authorizations and executive authorizations that have been renewed under this Ordinance during the report period further to 5 or more previous renewals;
- (vi) the respective numbers of applications for the issue of judge's authorizations, executive authorizations and emergency authorizations made under this Ordinance that have been refused during the report period;
- (vii) the respective numbers of applications for the renewal of judge's authorizations and executive authorizations made under this Ordinance that have been refused during the report period;
- (viii) the respective numbers of oral applications for the issue of judge's authorizations, executive authorizations and emergency authorizations made under this Ordinance that have been refused during the report period; and
- (ix) the respective numbers of oral applications for the renewal of judge's authorizations and executive authorizations made under this Ordinance that have been refused during the report period;

- (b) a list showing –
 - (i) the major categories of offences for the investigation of which prescribed authorizations have been issued or renewed under this Ordinance during the report period; and
 - (ii) the number of persons arrested during the report period as a result of or further to any interception or covert surveillance carried out pursuant to a prescribed authorization;
- (c) a list showing –
 - (i) the number of device retrieval warrants issued under this Ordinance during the report period, and the average duration of the warrants; and
 - (ii) the number of applications for the issue of device retrieval warrants made under this Ordinance that have been refused during the report period;
- (d) a list showing –
 - (i) a summary of reviews conducted by the Commissioner under section 40 during the report period;
 - (ii) the number and broad nature of any cases of abuses or suspected abuses, irregularities or errors identified in the reviews during the report period;
 - (iii) the number of applications for examination that have been received by the Commissioner during the report period;
 - (iv) the respective numbers of notices given by the Commissioner under section 43(2) and section 43(3) during the report period further to examinations;

- (iva) the number of cases in which a notice has been given by the Commissioner under section 46A during the report period;
- (v) the broad nature of recommendations made by the Commissioner under sections 49 and 50 during the report period;
- (vi) the number of cases in which information subject to legal professional privilege has been obtained in consequence of any interception or covert surveillance carried out pursuant to a prescribed authorization during the report period; and
- (vii) the number of cases in which disciplinary action has been taken in respect of any officer of a department according to any report submitted to the Commissioner under section 41, 46 or 50 during the report period, and the broad nature of such action; and

(e) an assessment on the overall compliance with the relevant requirements during the report period.

(3) The report is to be submitted within 6 months after the expiry of the report period.

(4) The Chief Executive shall cause to be laid on the table of the Legislative Council a copy of the report, together with a statement as to whether any matter has been excluded from that copy under subsection (5) without the agreement of the Commissioner.

(5) If the Chief Executive considers that the publication of any matter in the report referred to in subsection (4) would be prejudicial to the prevention or detection of crime or the protection of public security, he may, after consultation with the Commissioner, exclude such matter from the copy of the report to be laid on the table of the Legislative Council under that subsection.

(6) In this section, “report period” (報告期間), in relation to a report required to be submitted under subsection (1), means –

- (a) the period beginning on the commencement of this Ordinance and ending on 31 December in the same year; or
- (b) any of the succeeding periods of 12 months ending on 31 December.

48. Other reports to Chief Executive by Commissioner

In addition to any report required to be submitted to the Chief Executive under section 47, the Commissioner may from time to time submit any further report to the Chief Executive on any matter relating to the performance of his functions under this Ordinance as he thinks fit.

49. Recommendations to Secretary for Security on code of practice

(1) If, in the course of performing any of his functions under this Ordinance, the Commissioner considers that any provision of the code of practice should be revised to better carry out the objects of this Ordinance, he may make such recommendations to the Secretary for Security as he thinks fit.

(2) Where the Commissioner makes any recommendations to the Secretary for Security under subsection (1), the Secretary shall notify the Commissioner of any exercise of power by him under section 59(3) to implement the recommendations, as soon as reasonably practicable after the recommendations have been made or, where the Commissioner has specified any period for the issue of the notification when making the recommendations, within that period.

50. Recommendations to departments

(1) If, in the course of performing any of his functions under this Ordinance, the Commissioner considers that any arrangements made by any department should be changed to better carry out the objects of this Ordinance or the provisions of the code of practice,

he may make such recommendations to the head of the department as he thinks fit.

(2) Where the Commissioner makes any recommendations to the head of the department under subsection (1), the head of the department shall submit to the Commissioner a report with details of any measures taken by the department to implement the recommendations, as soon as reasonably practicable after the recommendations have been made or, where the Commissioner has specified any period for submission of the report when making the recommendations, within that period.

(3) Without prejudice to sections 47 and 48, the Commissioner may, whether before or after the head of the department has submitted a report to him under subsection (2), refer the recommendations and any other matters he thinks fit to the Chief Executive or the Secretary for Justice or both.

Division 5—Further Provisions Relating to Performance of Functions by Commissioner

51. Further powers of Commissioner

(1) For the purpose of performing any of his functions under this Ordinance, the Commissioner may—

(a) require any public officer or any other person to answer any question, and to provide any information, document or other matter in his possession or control to the Commissioner, within the time and in the manner specified by the Commissioner when making the requirement; and

(b) require any officer of a department to prepare any report on any case of interception or covert surveillance handled by the department, or on any class of such cases, within the time and in the manner specified by the Commissioner when making the requirement.

(2) Notwithstanding any other provision of this Ordinance or any other

law, any person on whom a requirement is imposed by the Commissioner under subsection (1) shall comply with the requirement.

(3) Subject to section 43 herein, ~~Except except~~ as otherwise provided in this Ordinance, the Commissioner shall not be required to produce in any court or to divulge or communicate to any court, or to provide or disclose to any person, any information, document or other matter compiled by, or made available to, him in the course of performing any of his functions under this Ordinance.

(4) Except as otherwise provided in this Ordinance, the Commissioner may determine the procedure to be adopted in performing any of his functions under this Ordinance.

52. General obligations of departments to report on non-compliance

Without prejudice to other provisions of this Part, where the head of any department considers that there may have been any case of failure by the department or any of its officers to comply with any relevant requirement, he shall submit to the Commissioner a report with details of the case.

53. Commissioner not regarded as court

In performing any of his functions under this Ordinance, the Commissioner is for all purposes not regarded as a court or a member of a court.

PART 5

FURTHER SAFEGUARDS

54A. Contravention of this Ordinance

In addition to any or all of the remedies herein provided, any contravention of this Ordinance shall be a civil wrong actionable in equitable relief as well as damages.

54. Regular reviews

(1) The head of each department shall make arrangements to keep under regular review the compliance by officers of the department with the relevant requirements.

(2) Without prejudice to subsection (1), where the head of any department has made any designation under section 7, he shall make arrangements for officers of a rank higher than those held by the authorizing officers of the department to keep under regular review the performance by the authorizing officers of any function under this Ordinance.

55. Discontinuance of interception or covert surveillance

(1) If, in the course of or further to any regular review conducted under section 54(1) or (2), the officer by whom the regular review is or has been conducted is of the opinion that any ground for discontinuance of a prescribed authorization exists, he shall, as soon as reasonably practicable after forming the opinion, cause the interception or covert surveillance concerned to be discontinued.

(2) Without prejudice to subsection (1), where a prescribed authorization has been issued or renewed under this Ordinance, the officer of the department concerned who is for the time being in charge of the interception or covert surveillance concerned—

(a) shall, as soon as reasonably practicable after he becomes aware that any ground for discontinuance of the prescribed authorization exists, cause the interception or covert surveillance to be discontinued; and

(b) may at any time cause the interception or covert surveillance to be discontinued.

(3) Where any officer has caused any interception or covert surveillance to be discontinued, whether under subsection (1) or (2), he shall, as soon as reasonably practicable after the discontinuance, cause a report on the discontinuance and the ground for the discontinuance to be provided to the relevant

authority to whom an application under this Ordinance for the issue or renewal of the prescribed authorization concerned has last been made.

(4) Where the relevant authority receives a report under subsection (3), he shall, as soon as reasonably practicable after receiving the report, revoke the prescribed authorization concerned.

(5) Where any prescribed authorization is revoked under subsection (4), the prescribed authorization is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.

(6) For the purposes of this section, a ground for discontinuance of a prescribed authorization exists if—

(a) the application for, issuance or renewal of any prescribed authorization was in contravention of this Ordinance;

(b) the interception or acts of covert surveillance carried out was in excess of the prescribed authorization;

(ac) the conditions for the continuance of the prescribed authorization under section 3 are not or are no longer met; or

(bd) the relevant purpose of the prescribed authorization has been achieved.

(7) In this section, “relevant duration provision” (有關時限條文) means section 10(b), 13(b), 16(b), 19(b) or 22(1)(b) (as may be applicable).

55A. Reports to relevant authorities following arrests

(1) A prescribed authorization ceases to have effect automatically upon the arrest of the subject of the interception or covert surveillance. The officer of the department concerned who is for the time being in charge of the interception or covert surveillance concerned shall, immediately after he becomes aware of the matter take all necessary steps to cease any interception or

covert surveillance being or would be carried out in respect of the arrested person.

(3) If, at the time of the provision of a report to the relevant authority under subsection (1), the relevant authority is no longer holding his office or performing the relevant functions of his office –

- (a) without prejudice to section 54 of the Interpretation and General Clauses Ordinance (Cap. 1), the reference to relevant authority in that subsection includes the person for the time being appointed as a panel judge or authorizing officer (as the case may be) and lawfully performing the relevant functions of the office of that relevant authority; and
- (b) the provisions of this section are to apply accordingly.

56. Safeguards for protected products

(1) Where any protected product has been obtained pursuant to any prescribed authorization issued or renewed under this Ordinance on an application by any officer of a department, the head of the department shall make arrangements to ensure –

- (a) that the following are limited to the minimum that is necessary for the relevant purpose of the prescribed authorization –
 - (i) the extent to which the protected product is disclosed;
 - (ii) the number of persons to whom any of the protected product is disclosed;
 - (iii) the extent to which the protected product is copied; and
 - (iv) the number of copies made of any of the protected product;

(b) that all practicable steps are taken to ensure that the protected product is protected against unauthorized or accidental access, processing, erasure or other use;

(ba) that any information or intelligence report or record generated from the protected product are subject to the same restriction and protection as the protected product; and

(c) that the protected product ~~that the protected product is destroyed as soon as its retention is not necessary for the relevant purpose of the prescribed authorization~~ and all information or intelligence report or record generated from it are destroyed as soon as its retention is not necessary for the relevant purpose of the prescribed authorization.

(1A) Where any protected product described in subsection (1) contains any communication that is subject to legal professional privilege, subsection (1)(c) is to be construed as also requiring the head of the department concerned to make arrangements to ensure that the person entitled to claim such legal professional privilege be notified of the same and to preserve the protected product pending the person's considering of what, any, action is to be taken as regards the same.

~~(2) For the purposes of this section, something is necessary for the relevant purpose of a prescribed authorization if—~~

~~(a) it continues to be, or is likely to become, necessary for the relevant purpose; or~~

~~(b) except in the case of a prescribed authorization for a telecommunications interception, it is necessary~~

~~for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted.~~

57. Record keeping

(1) Without prejudice to section 56, each department shall keep a record which is to contain—

(a) in respect of each application for the issue or renewal of a prescribed authorization under this Ordinance by any officer of the department, a record of—

(i) the application (including a copy of any affidavit or statement provided under Part 3 for the purposes of the application); and

(ii) the determination in respect of the application by the relevant authority (including a copy of any prescribed authorization issued or renewed under Part 3 as a result of the application);

(b) in respect of each application of confirmation of an emergency authorization by any officer of the department as provided for in section 23(1), a record of—

(i) the application (including a copy of any affidavit provided under section 23(2)(b) or, where section 28 applies, a copy of any record, affidavit or other document provided as described in section 28(1)(b), for the purposes of the application); and

(ii) the determination in respect of the application by a panel judge (including a copy of any endorsement made or, where section 28 applies, a copy of any emergency authorization issued, under section 24(5) as a result of the application);

(c) in respect of each application for confirmation of a prescribed authorization or renewal by any officer of the department as provided for in section 26(1), a record of—

(i) the application (including a copy of any record, affidavit or statement provided under section 26(2)(b) for the purposes of the application); and

(ii) the determination in respect of the application by the relevant authority (including a copy of any prescribed

- authorization issued or renewed under section 27(5) as a result of the application);
- (d) a record of—
- (i) any case in which any interception or covert surveillance has been discontinued by any officer of the department under section 55; and
 - (ii) any case in which any prescribed authorization has been revoked under section 55 further to the discontinuance;
- (e) in respect of each application for the issue of a device retrieval warrant under section 32 by any officer of the department, a record of—
- (i) the application (including a copy of any affidavit provided under section 32(2)(b) for the purposes of the application); and
 - (ii) the determination in respect of the application by a panel judge (including a copy of any device retrieval warrant issued under section 33(3) as a result of the application);
- (f) a record of—
- (i) any case to which section 23(3) applies by reason that no application for confirmation of an emergency authorization is made within the period of 48 hours by any officer of the department;
 - (ii) any case to which section 26(3) applies by reason that no application for confirmation of a prescribed authorization or renewal is made within the period of 48 hours by any officer of the department; and
 - (iii) any findings in respect of any other irregularities and errors identified or detected by any officer of the department, whether in any regular review conducted under section 54(1) and (2) or otherwise; and
- (g) any record reasonably required to be kept by the department to enable the Commissioner to prepare reports for submission to the Chief Executive under section 47, or otherwise to perform any of his functions under this Ordinance.
- (2) The record kept under subsection (1)—

(a) to the extent that it relates to any prescribed authorization or device retrieval warrant—

(i) is to be retained for a period of at least ~~2~~10 years after the day on which the prescribed authorization or device retrieval warrant (as the case may be) has ceased to have effect; and
(ii) without prejudice to subparagraph (i), where it has come to the notice of the department concerned that any relevant civil or criminal proceedings before any court are pending or are likely to be instituted, or any relevant review is being conducted under section 40, or, in the case of a prescribed authorization, any relevant application for an examination has been made under section 42, is to be retained—

(A) in the case of any pending proceedings, review or application, at least until the pending proceedings or application has been finally determined or finally disposed of or until the review has been completed or finally disposed of (as the case may be); or

(B) in the case of any proceedings which are likely to be instituted, at least until they have been finally determined or finally disposed of or, if applicable, until they are no longer likely to be instituted; or

(b) to the extent that it does not relate to any prescribed authorization or device retrieval warrant, is to be retained for a period of at least ~~2~~10 years.

(3) For the purposes of subsection (2), any proceedings, review or application is, in relation to any part of a record that relates to any prescribed authorization or device retrieval warrant, regarded as relevant if, but only if—

(a) the prescribed authorization or device retrieval warrant (as the case may be) is or may be relevant to the determination of any question for the purposes of the proceedings, review or application (as the case may be); or

(b) in the case of a prescribed authorization, any protected product obtained pursuant to the prescribed authorization is or may be

relevant to the determination of any question for the purposes of the proceedings, review or application (as the case may be).

58. Non-admissibility of telecommunications interception product

(1A) Nothing in this Ordinance shall authorize any conduct by any person which affects or may affect the right to a fair trial nor shall any judge or court or prosecutor be constrained or limited in any way in ordering or giving disclosure of any material including any protected product necessary for a fair trial.

(1) Subject to subsection (1A) and the right of any person charged with a criminal offence to apply to the court for disclosure of a telecommunications interception product, Any any telecommunications interception product shall not be admissible in evidence in any proceedings before any court other than to prove that a relevant offence has been committed.

(2) Subject to subsection (1A) and the right of any person charged with a criminal offence to apply to the court for disclosure of a telecommunications interception product, Any any telecommunications interception product, and any particulars as to a telecommunications interception carried out pursuant to a relevant prescribed authorization, shall not be made available to any party to any proceedings before any court (other than any such proceedings instituted for a relevant offence).

~~(3) In any proceedings before any court (other than any such proceedings instituted for a relevant offence), any evidence or question which tends to suggest any of the following matters shall not be adduced or asked—~~

~~(a) that an application has been made for the issue or renewal of a relevant prescribed authorization, or the issue of a relevant device retrieval warrant, under this Ordinance;~~

~~(b) that a relevant prescribed authorization has been issued or renewed, or a relevant device retrieval warrant has been issued, under this Ordinance;~~

~~(c) that any requirement has been imposed on any person to provide assistance for the execution of a relevant prescribed authorization or a relevant device retrieval warrant;~~

~~(d) that any information has been obtained pursuant to a relevant prescribed authorization.~~

(4) This section is not to be construed as prohibiting the disclosure of any information that continues to be available for disclosure, to the extent that—

~~(a) the disclosure is made to ensure that a person conducting the prosecution of any offence has the information he needs to determine what is required of him by his duty to secure the fairness of the trial of that offence; or~~

~~(b) the disclosure is made to a judge alone in a case in which the judge has ordered the disclosure to be so made to him.~~ and which is necessary for the purposes of a fair trial.

~~(5) A judge may only order a disclosure under subsection (4)(b) if he is satisfied that the disclosure is essential in the interests of justice.~~

~~(6) Where a judge orders a disclosure under subsection (4)(b), and in consequence of that disclosure he considers that it is essential in the interests of justice, he may direct the person conducting the prosecution of any offence to make for the purposes of the proceedings concerned any such admission of fact as the judge considers essential to secure the fairness of the trial of that offence.~~

~~(7) Notwithstanding subsection (6), no direction made under that subsection authorizes or requires anything to be done in contravention of subsections (1), (2) and (3).~~

(8) In this section—

“party” (一方), in relation to any criminal proceedings, includes the prosecution;

~~“relevant device retrieval warrant” (有關器材取出手令) means a device retrieval warrant for the retrieval of any of the devices authorized to be used under a relevant prescribed authorization;~~
~~“relevant offence” (有關罪行) means any offence constituted by the disclosure of any telecommunications interception product or of any information relating to the obtaining of any telecommunications interception product (whether or not there are other constituent elements of the offence);~~
 “relevant prescribed authorization” (有關訂明授權) means a prescribed authorization for a telecommunications interception;
 “telecommunications interception product” (電訊截取成果) means any interception product to the extent that it is—
 (a) any contents of a communication that have been obtained pursuant to a relevant prescribed authorization; or
 (b) a copy of such contents.

59. Code of practice

(1) The Secretary for Security shall issue a code of practice for the purpose of providing practical guidance to officers of the departments in respect of matters provided for in this Ordinance.

(2) Without limiting the generality of subsection (1), the Secretary for Security may in the code of practice specify the form of any application to be made to a panel judge under this Ordinance.

(3) The Secretary for Security may from time to time revise the whole or any part of the code of practice, in a manner consistent with his power to issue the code under this section, and, unless the context otherwise requires, any reference to the code of practice, whether in this Ordinance or otherwise, is to be construed as a reference to the code as so revised.

(4) Any officer of a department shall, in performing any function under or for the purposes of any provision of this Ordinance, have regard to the provisions of the code of practice.

(5) A failure on the part of any person to comply with any provision of the code of practice—

(a) is for all purposes not of itself to be regarded as a failure to comply with any provision of this Ordinance; and

(b) without prejudice to paragraph (a), does not affect the validity of any prescribed authorization or device retrieval warrant.

PART 6

MISCELLANEOUS

60. Prescribed authorizations and device retrieval warrants not affected by minor defects

(1) A prescribed authorization or device retrieval warrant is not affected by any minor defect in it.

(2) Without prejudice to the generality of subsection (1), any information (including any protected product) obtained pursuant to a prescribed authorization is not by reason only of any minor defect in the prescribed authorization to be rendered inadmissible in evidence in any proceedings before any court.

(3) For the purposes of this section, any reference to minor defect, in relation to a prescribed authorization or device retrieval warrant, includes any defect or irregularity, other than a substantial defect or irregularity, in or in connection with—

(a) the issue, or the purported issue, of that prescribed authorization or device retrieval warrant or of a document purporting to be that prescribed authorization or device retrieval warrant; or

(b) the execution, or the purported execution, of that prescribed authorization or device retrieval warrant or of a document purporting to be that prescribed authorization or device retrieval warrant.

61. Immunity

(1) Subject to subsection (2), a person shall not incur any civil or criminal liability by reason only of—

(a) any conduct carried out pursuant to a prescribed authorization or device retrieval warrant (including any conduct incidental to such conduct);

(b) his performance or purported performance in good faith of any function under this Ordinance; or

(c) his compliance with a requirement made or purportedly made under this Ordinance.

(2) Nothing in subsection (1) affects any liability that is or may be incurred by any person by reason only of—

(a) any entry onto any premises without permission; or

(b) any interference with any property without permission.

62. Regulation

The Chief Executive in Council may make regulation for—

(a) the better carrying out of the purposes of this Ordinance; and

(b) without limiting the generality of paragraph (a), prescribing any matter which this Ordinance provides is, or may be, prescribed by regulation made under this section.

63. Amendment of Schedules

The Chief Executive in Council may, by notice published in the Gazette, amend Schedules 1, 2, 3 and 4.

64. Repeal and consequential amendments

(1) The Interception of Communications Ordinance (Cap. 532) is repealed.

(2) The enactments specified in Schedule 5 are amended as set out in that Schedule.

65. Transitional arrangements

(1A) Nothing in this Ordinance shall be construed as authorizing or permitting or applying to any interception of communications or

surveillance which has been held unlawful by any court before the commencement of this Ordinance.

(1)Subject to subsection (1A). ~~Where~~ where any materials have been obtained by or on behalf of any department by carrying out any telecommunications interception pursuant to an order issued or renewed before the commencement of this Ordinance under the provision then in force as section 33 of the Telecommunications Ordinance (Cap. 106), sections 56 and 58 apply, with necessary modifications, to the materials, to the extent that they are any of the contents of the communication intercepted or a copy of such contents, and to the relevant matters as if—

(a) the order were a prescribed authorization issued or renewed under this Ordinance, and accordingly—

- (i) the materials were, for the purposes of sections 56 and 58 respectively, protected product and telecommunications interception product; and
 - (ii) the application for the issue or renewal of the order were an application for the issue or renewal of a prescribed authorization under this Ordinance; and
- (b) the purpose sought to be furthered by carrying out the operation required to be carried out under the order were the relevant purpose of the order.
- (2) Subsection (1) is in addition to and not in derogation of section 23 of the Interpretation and General Clauses Ordinance (Cap. 1).
- (3) In this section—
- “copy” (文本), in relation to any contents of a communication referred to in subsection (1), means any of the following (whether or not in documentary form)—
- (a) any copy, extract or summary of such contents which identifies itself as such copy, extract or summary of such contents;
 - (b) any record referring to the telecommunications interception referred to in subsection (1) which is a record of the identity of any person who is the sender or intended recipient of the communication;
- “relevant matters” (有關事宜)—
- (a) in relation to section 58(2), means any particulars as to the telecommunications interception referred to in subsection (1); and
 - (b) in relation to section 58(3), means any evidence or question which tends to suggest any of the following matters—
 - (i) that an application has been made for the issue or renewal of the order referred to in subsection (1);
 - (ii) that the order has been issued or renewed;
 - (iii) that any requirement has been imposed on any person to provide assistance for the execution of the order;
 - (iv) that any information has been obtained pursuant to the order.

SCHEDULE 1 [ss. 2 & 63]

DEPARTMENTS

PART 1

DEPARTMENTS SPECIFIED FOR INTERCEPTION, ETC.

1. Customs and Excise Department
2. Hong Kong Police Force
3. Independent Commission Against Corruption

PART 2

DEPARTMENTS SPECIFIED FOR COVERT SURVEILLANCE, ETC.

1. Customs and Excise Department
 2. Hong Kong Police Force
 3. Immigration Department
 4. Independent Commission Against Corruption
-

SCHEDULE 2 [ss. 2, 6 & 63]

PROCEDURES OF, AND OTHER MATTERS RELATING TO, PANEL JUDGE

Judge' s Authorization

~~1. Provisions for consideration of applications
by panel judge to the High Court~~

~~(1) A panel judge court shall consider any application made to him
under this Ordinance in private.~~

~~(2) Without prejudice to subsection (1), the application may, where the panel judgecourt so directs, be considered at any place other than within the court precincts.~~

~~(3) Without prejudice to Division 5 of Part 3 of this Ordinance, nothing in this section prevents consideration of the application by the panel judgecourt on the basis of written submissions made to him.~~

~~2. Further powers of panel judgecourt~~

~~For the purpose of performing any of his functions under this Ordinance, a panel judgecourt may administer oaths and take affidavits.~~

3. Provisions for documents and records compiled by or made available to panel judge

(1) A panel judge shall cause all documents and records compiled by, or made available to, him for any purpose related to the performance of any of his functions under this Ordinance to be kept in a packet sealed by his order, as soon as they are no longer immediately required for the purpose of performing any of his functions under this Ordinance.

(2) Notwithstanding subsection (1), a panel judge to whom any documents or records are made available in the circumstances described in that subsection shall—

(a) cause a copy of each of the documents or records so made available to him to be certified by affixing his seal to it and signing on it; and

(b) cause the copy so certified to be made available to the department concerned.

(3) Where any documents or records are kept in a packet under subsection (1)—

(a) the packet is to be kept in a secure place specified by a panel judge;

(b) the packet may not be opened, and the documents or records may not be removed from the packet, except pursuant to an order

of a panel judge made for the purpose of performing any of his functions under this Ordinance; and

(c) the packet, and the documents or records, may not be destroyed except pursuant to an order of a panel judge.

(4) Where any packet is opened pursuant to any order of a panel judge referred to in subsection (3)(b)—

(a) if any documents or records have been removed from the packet, the panel judge shall cause the documents or records to be returned to be kept in the packet, as soon as they are no longer immediately required for the purpose of performing any of his functions under this Ordinance; and

(b) the panel judge shall cause the packet to be sealed by his order, as soon as access to the documents or records kept in it is no longer immediately required for the purpose of performing any of his functions under this Ordinance, and the provisions of subsection (3) apply, with necessary modifications, to the packet so sealed as they apply to the packet referred to in subsection (1).

(5) Nothing in this section prevents any of the documents and records referred to in subsection (1), or any copies of such documents and records, to be made available to the department concerned for the purposes of any relevant written determination provision or otherwise pursuant to an order of a panel judge.

(6) In this section, “relevant written determination provision” (有關書面決定條文) means section 9(3), 12(3), 24(5) (whether with or without reference to section 28 of this Ordinance), 27(5) or 33(3) of this Ordinance.

~~4. Panel judge to act judicially but not regarded as court~~

~~In performing any of his functions under this Ordinance, a panel judge shall act judicially and have the same powers, protection and immunities as a judge of the Court of First Instance has in relation to proceedings in that Court, although he is for all purposes not regarded as a court or a member of a court.~~

SCHEDULE 3 [ss. 8, 11, 14, 17, 20 & 63]

REQUIREMENTS FOR AFFIDAVIT OR STATEMENT FOR
APPLICATION FOR ISSUE OR RENEWAL OF PRESCRIBED
AUTHORIZATION FOR INTERCEPTION OR COVERT
SURVEILLANCE

PART 1

APPLICATION FOR ISSUE OF JUDICIAL AUTHORIZATION
FOR INTERCEPTION

An affidavit supporting an application for the issue of a judge' s
~~judicial~~ authorization for interception is to—

(a) state which of the purposes specified in section 3(1)(a)(i) and
(ii) of this Ordinance is sought to be furthered by carrying out the
interception and identify the serious crime sought to be prevented
or detected or the threat to public security, whichever is applicable;

(b) set out—

(i) the form of the interception and the information sought to
be obtained by carrying out the interception;
(ii) ~~if known~~, the identity of any person who is to be the
subject of the interception;
(iii) ~~if known~~, particulars of the addresses, numbers,
apparatus or other factors, or combination of factors, that are
to be used for identifying any communication that is to be
intercepted;

(iv) the proposed duration of the interception;

(v) the nature of, and an assessment of the immediacy and
gravity of—

(A) where the purpose sought to be furthered by
carrying out the interception is that specified in section
3(1)(a)(i) of this Ordinance, the serious crime to be
prevented or detected; or

(B) where the purpose sought to be furthered by
carrying out the interception is that specified in section

- 3(1)(a)(ii) of this Ordinance, the particular threat to public security; (vi) the benefits likely to be obtained by carrying out the interception;
- (vii) an assessment of the impact (if any) of the interception on any person other than that referred to in subparagraph (ii);
- (viii) the likelihood that any information-communication which may be subject to legal professional privilege, or may be confidential journalistic information, or sensitive personal information will be obtained by carrying out the interception; and
- (ix) the reason why the purpose sought to be furthered by carrying out the interception cannot reasonably be furthered by other less intrusive means;
- (x) set out all facts and matters in support of the reasonable suspicion specified in section 3 including the source of information or belief
- (xi) set out whether the subject of the interception has a criminal record, specifying the offences, if applicable
- and
- (c) identify by name and rank the applicant.

PART 2

APPLICATION FOR ISSUE OF JUDICIAL-JUDGE' S AUTHORIZATION FOR TYPE 1 SURVEILLANCE

An affidavit supporting an application for the issue of a judicial authorization for Type 1 surveillance is to—

- (a) state which of the purposes specified in section 3(1)(a)(i) and (ii) of this Ordinance is sought to be furthered by carrying out the Type 1 surveillance and identify the serious crime sought to be prevented or detected or the threat to public security, whichever is applicable;
- ;
- (b) set out—

- (i) the form of the Type 1 surveillance (including the kind or kinds of any devices to be used) and the information sought to be obtained by carrying out the Type 1 surveillance;
- (ii) ~~if known~~, the identity of any person who is to be the subject of the Type 1 surveillance;
- (iii) the identity of any person, other than that referred to in subparagraph (ii), who may be affected by the Type 1 surveillance or, if the identity of such person is not known, the description of any such person or class of such persons who may be affected by the Type 1 surveillance;
- (iv) ~~if known~~, particulars of any premises or any object or class of objects in or on or from which the Type 1 surveillance is to be carried out;
- (v) the proposed duration of the Type 1 surveillance;
- (vi) the nature of, and an assessment of the ~~immediacy~~ imminence and gravity of—
 - (A) where the purpose sought to be furthered by carrying out the Type 1 surveillance is that specified in section 3(1)(a)(i) of this Ordinance, the serious crime to be prevented or detected; or
 - (B) where the purpose sought to be furthered by carrying out the Type 1 surveillance is that specified in section 3(1)(a)(ii) of this Ordinance, the particular threat to public security;
- (vii) the benefits likely to be obtained by carrying out the Type 1 surveillance;
- (viii) an assessment of the impact (if any) of the Type 1 surveillance on any person referred to in subparagraph (iii);
- (ix) the likelihood that any information which may be subject to legal professional privilege, any confidential journalistic information or sensitive personal information will be obtained by carrying out the Type 1 surveillance; and
- (x) the reason why the purpose sought to be furthered by carrying out the Type 1 surveillance cannot reasonably be furthered by other less intrusive means;

- (x) set out all matters and facts in support of the reasonable suspicion specified in section 3 including the source of information or belief
- (xi) set out whether the subject of the interception has a criminal record, specifying the offences, if applicable
- and
- (c) identify by name and rank the applicant.

PART 3 APPLICATION FOR ISSUE OF EXECUTIVE AUTHORIZATION FOR TYPE 2 SURVEILLANCE

A statement supporting an application for the issue of an executive authorization for Type 2 surveillance is to—

(a) state which of the purposes specified in section 3(1)(a)(i) and (ii) of this Ordinance is sought to be furthered by carrying out the Type 2 surveillance and identify the serious crime sought to be prevented or detected or the threat to public security, whichever is applicable ;

(b) set out—

(i) the form of the Type 2 surveillance (including the kind or kinds of any devices to be used) and the information sought to be obtained by carrying out the Type 2 surveillance;

(ii) if known, the identity of any person who is to be the subject of the Type 2 surveillance;

(iii) the identity of any person, other than that referred to in subparagraph (ii), who may be affected by the Type 2 surveillance or, if the identity of such person is not known, the description of any such person or class of such persons who may be affected by the Type 2 surveillance;

(iv) if known, particulars of any premises or any object or class of objects in or on which the Type 2 surveillance is to be carried out;

(v) the proposed duration of the Type 2 surveillance;

(vi) the nature of, and an assessment of the immediacy and gravity of—

(A) where the purpose sought to be furthered by carrying out the Type 2 surveillance is that specified in section 3(1)(a)(i) of this Ordinance, the serious crime to be prevented or detected; or

(B) where the purpose sought to be furthered by carrying out the Type 2 surveillance is that specified in

- section 3(1)(a)(ii) of this Ordinance, the particular threat to public security;
- (vii) the benefits likely to be obtained by carrying out the Type 2 surveillance;
- (viii) an assessment of the impact (if any) of the Type 2 surveillance on any person referred to in subparagraph (iii);
- (ix) the likelihood that any information which may be subject to legal professional privilege will be obtained by carrying out the Type 2 surveillance; and
- (x) the reason why the purpose sought to be furthered by carrying out the Type 2 surveillance cannot reasonably be furthered by other less intrusive means;
- (x) set out all facts and all matters in support of the reasonable suspicion specified in section 3 including the source of information or belief
- (xi) set out whether the subject of the interception has a criminal record, specifying the offences, if applicable
- and
- (c) identify by name and rank the applicant.

PART 4

APPLICATION FOR RENEWAL OF ~~JUDICIAL~~ JUDGE' S AUTHORIZATION OR EXECUTIVE AUTHORIZATION FOR INTERCEPTION OR COVERT SURVEILLANCE

An affidavit or statement supporting an application for the renewal of a judicial authorization for interception or Type 1 surveillance or an executive authorization for Type 2 surveillance is to—

- (a) set out—
 - (i) whether the renewal sought is the first renewal and, if not, each occasion on which the judicial authorization or executive authorization has been renewed previously;

- (ii) any significant change to any information previously provided in any affidavit or statement under this Ordinance for the purposes of any application for the issue or renewal of the judicial authorization or executive authorization, or for the purposes of any application made further to an oral application for confirmation of the judicial authorization or executive authorization or its previous renewal;
 - (iii) the value of the information so far obtained pursuant to the judicial authorization or executive authorization;
 - (iv) the reason why it is necessary to apply for the renewal; and
 - (v) the proposed duration of the interception, Type 1 surveillance or Type 2 surveillance (as the case may be); and
- (b) identify by name and rank the applicant.
-

SCHEDULE 4 [ss. 32 & 63]

REQUIREMENTS FOR AFFIDAVIT FOR APPLICATION FOR ISSUE OF DEVICE RETRIEVAL WARRANT

An affidavit supporting an application for the issue of a device retrieval warrant for the retrieval of any of the devices authorized to be used under a prescribed authorization is to—

- (a) set out—
 - (i) the kind or kinds of the devices sought to be retrieved;
 - (ii) particulars of the premises or object from which the devices are to be retrieved, and the reason why the applicant considers that the devices are in or on such premises or object;
 - (iii) the estimated time required to complete the retrieval;
 - (iv) an assessment of the impact (if any) of the retrieval on any person; and
 - (v) the need for the retrieval; and
- (b) identify by name and rank the applicant.

SCHEDULE 5 [s. 64]

CONSEQUENTIAL AMENDMENTS

Post Office Ordinance

1. Warrant of Chief Secretary for Administration
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, 12 or 13

(1) Section 14 is amended, in the heading, by repealing “, 12 or 13” and substituting “or 12”.

(2) Section 14 is amended by repealing “, 12 or 13” and substituting “or 12”.

3. Extension of sections 12, 13 and 14 to articles not transmissible
by post

(1) Section 15 is amended, in the heading, by repealing “, 13”.

(2) Section 15 is amended by repealing “, 13”.

Post Office Regulations

4. Regulation amended

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

Telecommunications Ordinance

5. Section substituted

Section 33 of the Telecommunications Ordinance (Cap. 106) is repealed and the following substituted—

“33. Orders for interception of messages for provision of facilities

(1) For the purpose of providing or making available facilities reasonably required for—

(a) the detection or discovery of any telecommunications service provided in contravention of any provision of this Ordinance or any regulation made under this Ordinance or any of the terms or conditions of a licence granted under this Ordinance; or

(b) the execution of prescribed authorizations for telecommunications interception that may from time to time be issued or renewed under the Interception of Communications and Surveillance Ordinance (of 2006), the Chief Executive may order that any class of messages shall be intercepted.

(2) An order under subsection (1) shall not of itself authorize the obtaining of the contents of any individual message.

(3) In this section—

“contents” (内容), in relation to any message, has the meaning assigned to it in section 2(5) of the Interception of Communications and Surveillance Ordinance (of 2006) in relation to a communication referred to in that section;

“prescribed authorization” (訂明授權) has the meaning assigned to it in section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

“telecommunications interception” (●●●●●●) has the meaning assigned to it in section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006).”.

Prevention of Bribery Ordinance

6. Public bodies

Schedule 1 to the Prevention of Bribery Ordinance (Cap. 201) is amended by adding—

“107. Commissioner on Interception of Communications and Surveillance.”.

Personal Data (Privacy) Ordinance

7. Section added

The Personal Data (Privacy) Ordinance (Cap. 486) is amended by adding—

“58A. Protected product and relevant records under Interception of Communications and Surveillance Ordinance

(1) A personal data system is exempt from the provisions of this Ordinance to the extent that it is used by a data user for the collection, holding, processing or use of personal data which are, or are contained in, protected product or relevant records.

(2) Personal data which are, or are contained in, protected product or relevant records are exempt from the provisions of this Ordinance.

(3) In this section—

“device retrieval warrant” (器材取出手令) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

“prescribed authorization” (訂明授權) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

“protected product” (受保護成果) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

“relevant records” (有關紀錄) means documents and records relating to—

(a) any application for the issue or renewal of any prescribed authorization or device retrieval warrant under the Interception of Communications and Surveillance Ordinance (of 2006); or

(b) any prescribed authorization or device retrieval warrant issued or renewed under that Ordinance (including anything done pursuant to or in relation to such prescribed authorization or device retrieval warrant).”.

Official Secrets Ordinance

8. Information related to commission of offences and criminal investigations

Section 17(2)(c), (d) and (e) of the Official Secrets Ordinance (Cap. 521) is repealed and the following substituted—

“(c) any information, document or article which is interception product within the meaning of the Interception of Communications and Surveillance Ordinance (of 2006); or

(d) any information relating to the obtaining of any interception product described in paragraph (c).”.

Explanatory Memorandum

The object of this Bill is to regulate the conduct of interception of communications and the use of surveillance devices by or on behalf of public officers.

2. The Bill contains 6 Parts and 5 Schedules.

Part 1—Preliminary

3. Part 1 provides for preliminary matters—

(a) Clause 2 contains the definitions with reference to which the provisions of the Bill are to be interpreted. In particular—

(i) “interception” is defined to mean the carrying out of any intercepting act in respect of communications, and for that purpose—

— “communication” is defined to mean any communication transmitted by a postal service or by a telecommunications system; and

— “intercepting act” is defined to mean the inspection of any of the contents of a communication, in the course of its transmission, by persons other than its sender or its intended recipient;

(ii) “covert surveillance” is defined to mean systematic surveillance carried out with the use of any surveillance device for the purposes of a specific investigation or operation where, among other conditions that apply, any

person who is the subject of the surveillance is entitled to a reasonable expectation of privacy; and, for the purposes of the Bill, covert surveillance is further divided into “Type 1 surveillance” and “Type 2 surveillance” as defined under their respective definitions; and

(iii) “department” is defined, in relation to interception cases, to mean the Customs and Excise Department, the Hong Kong Police Force, and the Independent Commission Against Corruption, and, in relation to covert surveillance cases, to mean the same departments as well as the Immigration Department.

(b) Clause 3 sets out the conditions for the issue or renewal, or the continuance, of prescribed authorizations under the Bill. Under those conditions, any interception or covert surveillance sought to be authorized should be carried out for the purpose of preventing or detecting serious crime or for the purpose of protecting public security, and should, upon taking into consideration various specified matters, also be proportionate to such purpose.

Part 2—Prohibition on Interception and Covert Surveillance

4. Part 2 contains the prohibition provisions—

(a) Clause 4 provides that no public officers shall, directly or through any other person, carry out any interception. This prohibition does not apply if the interception is carried out pursuant to a prescribed authorization, or is carried out in respect of telecommunications transmitted by specified radiocommunications, or is otherwise authorized, permitted or required to be carried out under any other enactments.

(b) Clause 5 provides that no public officers shall, directly or through any other person, carry out any covert surveillance. This prohibition does not apply if the covert surveillance is carried out pursuant to a prescribed authorization.

Part 3—Prescribed Authorizations, etc.

5. Part 3 contains provisions relating to prescribed authorization, and is divided into 6 Divisions—

(a) Division 1 (clauses 6 and 7) provides for the appointment and designation of panel judges and authorizing officers, being relevant authorities having functions to approve applications for the issue or renewal of prescribed authorizations, etc. under

Part 3—

(i) ~~Clause 6 provides for the appointment of 3 to 6 eligible judges as panel judges by the Chief Executive on the recommendation of the Chief Justice. It also p~~Provides that Schedule 2 applies to the procedures and other matters relating to panel judges.

(ii) Clause 7 provides for the designation of officers not below a rank equivalent to that of senior superintendent of police as authorizing officers by the head of the departments.

(b) Division 2 (clauses 8 to 13) provides for the issue of judicial authorizations for interception or Type 1 surveillance, on the application to a panel judge by an officer of a department with the approval of a directorate officer of that department, and further for the renewal of judicial authorizations. Subject to the conditions set out in clause 3, a judicial authorization may be issued or renewed for a maximum term of 3 months.

(c) Division 3 (clauses 14 to 19) provides for the issue of executive authorizations for Type 2 surveillance, on the application to an authorizing officer of a department by an officer of that department, and further for the renewal of executive authorizations. Subject to the conditions set out in clause 3, an executive authorization may be issued or renewed for a maximum term of 3 months.

(d) Division 4 (clauses 20 to 24) provides for the issue of emergency authorizations for interception or Type 1 surveillance by the head of departments in any emergency cases where it is not practicable for judicial authorizations to be obtained from panel judges. However, while the conditions set out in clause 3 also

apply to the issue of the emergency authorization, the emergency authorization is only to last for a maximum term of 48 hours and in any event is subject to confirmation on an application to a panel judge by an officer of the department concerned. Where the panel judge does not confirm the emergency authorization, he may order the revocation or variation of the emergency authorization, and may also order the destruction of any of the information obtained pursuant to the emergency authorization.

(e) Division 5 (clauses 25 to 28) provides for the alternative of making oral applications for the issue or renewal of prescribed authorizations in specified circumstances, notwithstanding the requirements for written applications otherwise applicable to prescribed authorizations under Part 3. Where any oral application is made, supporting information may be provided orally, and the determination in respect of the application may also be delivered orally. However, the determination under an oral authorization is also subject to confirmation on an application to the relevant authority by whom the oral application has been determined. Where the relevant authority does not confirm the prescribed authorization or the renewal issued or granted under the determination, he may order the revocation or variation of the prescribed authorization or renewal, and may also order the destruction of any of the information obtained pursuant to the prescribed authorization or renewal.

(f) Division 6 (clauses 29 to 37) contains general provisions applicable to prescribed authorizations. Clauses 29 to 31 deal with matters that may be authorized, required or provided for by prescribed authorizations. Clauses 32 to 37 then provide for the issue, after a prescribed authorization has ceased to have effect, of a device retrieval warrant for the retrieval of devices previously installed in or on premises or objects pursuant to the prescribed authorization. The application is to be made to a panel judge by an officer of a department, and on considering the application, the panel judge may issue a device retrieval warrant for a maximum term of 3 months.

Part 4—The Commissioner

6. Part 4 contains provisions relating to the Commissioner on Interception of Communications and Surveillance, and is divided into 5 Divisions—

(a) Division 1 (clauses 38 and 39) provides for the establishment of the office of the Commissioner and for his functions. The Commissioner is to be appointed by the Chief Executive on the recommendation of the Chief Justice. His functions are to oversee the compliance by departments and their officers with the relevant requirements (cf. definition of “relevant requirement” in clause 2), and in particular to perform functions set out in Divisions 2 to 4, and other functions prescribed by regulation made under clause 62 and generally by the Bill and by other enactments.

(b) Division 2 (clauses 40 and 41) provides for reviews conducted by the Commissioner on compliance by departments and their officers with the relevant requirements. The Commissioner is also to notify departments concerned of any case where he has made any findings that there has been failure by any department or any of its officers to comply with any relevant requirement.

(c) Division 3 (clauses 42 to 46) provides for examinations carried out by the Commissioner, on the application by any person who believes that he is the subject of any interception or covert surveillance carried out by a department. The Commissioner is to consider the case by adopting the judicial review principles and by reference to written submissions made to him. After consideration of the case, he is to notify the applicant whether he has found the case in the applicant’s favour, and may, if he thinks fit, make an order for the payment by the Government to the applicant of a sum of compensation, which may include compensation for injury to feelings. The Commissioner is also to notify the department concerned of any case where he has found the case in the applicant’s favour.

(d) Division 4 (clauses 47 to 50) provides for the submission by the Commissioner to the Chief Executive of annual reports containing

specified information, and then requires a copy of the reports to be laid on the table of the Legislative Council. The Commissioner may also from time to time make further reports to the Chief Executive, and may also make recommendations to the Secretary for Security and the departments on specified matters. (e) Division 5 (clauses 51 to 53) contains further provisions relating to the performance of functions by the Commissioner. The Commissioner may impose requirements on public officers and other persons to provide information to him, and may require officers of departments to prepare reports in respect of cases of interception or covert surveillance handled by the departments. In addition, the head of a department is to keep the Commissioner informed of any case in which he considers that there may have been any case of failure by the department or any of its officers to comply with any relevant requirement.

Part 5—Further Safeguards

7. Part 5 provides for further safeguards in respect of interception and covert surveillance carried out by departments—

(a) Under clauses 54 and 55, a department is to conduct regular reviews on the compliance by officers of the department with the relevant requirements, and on the performance by authorizing officers of the department of any function under the Bill. Any interception or covert surveillance carried out pursuant to a prescribed authorization is to be discontinued once the officer by whom a regular review is conducted, or the officer in charge of the operation, considers that the conditions set out in clause 3 are not met, or that the relevant purpose of the prescribed authorization has been achieved (cf. definition of “relevant purpose” in clause 2). In addition, the officer in charge of the operation may at any time cause the operation to be discontinued. In any case where any operation is discontinued, the relevant authority by whom the prescribed authorization authorizing the operation has been issued or renewed is to be notified, and then to revoke the prescribed authorization.

(b) Under clause 56, each department shall make arrangements to ensure that any product obtained pursuant to a prescribed authorization (cf. definition of “protected product” in clause 2) is to be dealt with in accordance with specified arrangements, in order to minimize the extent to which the product is disclosed or copied, or subject to unauthorized or accidental access, processing, erasure or other use, and to ensure its timely destruction.

(c) Under clause 57, each department is also to keep a proper record in respect of specified matters, including matters relating to applications for the issue or renewal of prescribed authorizations or device retrieval warrants, and other matters provided for in the Bill. The record is, to the extent that it relates to any prescribed authorization or device retrieval warrant, to be kept for a minimum term of 2 years after the prescribed authorization or device retrieval warrant ceases to have effect, and is in any event to be kept at least until any relevant pending or anticipated proceedings, etc. have been finally disposed of. The part of the record that relates to other matters is to be kept for a minimum term of 2 years.

(d) By virtue of clause 58, in any proceedings before any court (other than proceedings for specified offences (cf. definition of “relevant offence” in clause 58)), any product obtained pursuant to a prescribed authorization for interception of a communication transmitted by a telecommunications system (cf. definition of “telecommunications interception product” in clause 58) shall not be admissible in evidence and shall not be made available to any party, and any evidence or question which tends to suggest matters relating to any application for the issue or renewal of any relevant prescribed authorizations, and other related matters shall not be adduced or asked. However, the clause also provides that it does not prohibit disclosure in specified cases where the disclosure is required in the interests of justice, etc.

(e) Clause 59 further provides that the Secretary for Security is to issue a code of practice for the purpose of providing practical guidance to officers of the departments in respect of matters provided for in the Bill.

Part 6—Miscellaneous

8. Part 6 contains miscellaneous provisions dealing with minor defects of prescribed authorizations and device retrieval warrants, immunity, regulation, and amendment of schedules. In addition, clause 64 seeks to repeal the Interception of Communications Ordinance (Cap. 532) and to introduce consequential amendments to ordinances including the Post Office Ordinance (Cap. 98), the Telecommunications Ordinance (Cap. 106) and other appropriate ordinances. Further, clause 65 provides for a transitional arrangement so that, among other matters, any materials obtained by way of interception pursuant to an order issued or renewed under section 33 of the Telecommunications Ordinance (Cap. 106) before the commencement of the Bill as enacted are also subject to clauses 56 and 58 as if they were product obtained pursuant to a prescribed authorization.

《Interception of Communications and Covert Surveillance Bill》

Further amendments proposed by Hon. Margaret Ng

Clause	Proposed amendment
New	<p>By adding –</p> <p>“66. Sunset</p> <p>(1) Subject to subsection (2), Section 4(2), (3) and Section 5(2) of Part 2 and all provisions in Part 3 of this Ordinance shall cease to have effect on 8 August 2008.</p> <p>(2) Any prescribed authorization issued, renewed or confirmed, any retrieval warrant issued, and any authorization for other matters contained in the prescribed authorization prior to 8 August 2008 is deemed to expire on that date.</p> <p>(3) No later than 15 months prior to 8 August 2008, the Commissioner shall conduct a full and independent public consultation on the provisions and implementation of this Ordinance, and their effect on the freedom of private communications provided under Article 30 of the Basic Law. The Commissioner shall state the findings of the consultation and his recommendations on the revision or replacement of this Ordinance in a report to the Chief Executive.</p> <p>(4) The Commissioner’s report referred to in subsection (3) shall be laid on the table of the Legislative Council no later than 10 months prior to 8 August 2008.</p> ”

INTERCEPTION OF COMMUNICATIONS AND
SURVEILLANCE BILL

Committee Stage Amendments proposed by Hon James To as positioned July 14, 2006.
The CSAs are in bold italics and double crossing (in case of deletion) for Members' ease of reference.

A BILL

To

Regulate the conduct of interception of communications and the use of surveillance devices by or on behalf of public officers and to provide for related matters.

Enacted by the Legislative Council.

PART 1
PRELIMINARY

1. Short title

This Ordinance may be cited as the Interception of Communications and Surveillance Ordinance.

2. Interpretation

- (1) In this Ordinance, unless the context otherwise requires –
- “address” (地址), in relation to a communication transmitted by a postal service, includes a postal box address;
- ~~“authorizing officer” (授權人員), in relation to any department, means any officer designated under section 7 by the head of the department to be an authorizing officer;~~
- “code of practice” (實務守則) means the code of practice issued under section 59;
- “Commissioner” (專員) means the Commissioner on Interception of Communications and Surveillance appointed under section 38;
- “communication” (通訊) means –
- (a) any communication transmitted by a postal service; or
- (b) any communication transmitted by a telecommunications system;
- “communication transmitted by a postal service” (藉郵政服務傳送的通訊) includes a postal article;
- “conduct” (行為) includes any act or omission, and any series of acts or omissions or of acts and omissions;
- “conveyance” (運輸工具) means any vehicle, vessel, aircraft, hovercraft or other

conveyance;

“copy” (文本) –

- (a) in relation to any contents of a communication that have been obtained pursuant to a prescribed authorization for interception, means any of the following (whether or not in documentary form) –
 - (i) any copy, extract or summary of such contents ~~which identifies itself as such copy, extract or summary of such contents;~~
 - (ii) any record referring to the interception which is a record of the identity of any person who is the sender or intended recipient of the communication; or
- (b) in relation to any material that has been obtained pursuant to a prescribed authorization for covert surveillance, means any of the following (whether or not in documentary form) –
 - (i) any copy, extract or summary of the material ~~which identifies itself as such copy, extract or summary of the material;~~
 - (ii) any transcript or record made of the material ~~which identifies itself as such transcript or record made of the material;~~

“court” (法院), without prejudice to sections 6(3A) and 53 ~~53 and section 4 of Schedule 2~~ –

- (a) means a court as defined in section 3 of the Interpretation and General Clauses Ordinance (Cap. 1); and
- (b) includes a magistrate and a tribunal;

“covert surveillance” (秘密監察) –

- (a) means any ~~systematic~~ surveillance carried out with the use of any surveillance device or by an undercover agent or by any person on the instruction of or under the control of or with the cooperation of an officer of a department specified in Schedule 1 for the purposes of a specific investigation or operation, if the surveillance –
 - (i) is carried out in circumstances where any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy;
 - (ii) is carried out in a manner calculated to ensure that the person is unaware that the surveillance is or may be taking place; and
 - (iii) is likely to result in the obtaining of any private information about the person; but
- (b) does not include ~~any such systematic surveillance to the extent that it constitutes interception under this Ordinance; –~~
 - (i) any spontaneous reaction to unforeseen events or circumstances; and
 - (ii) any such surveillance that constitutes interception under this Ordinance;

“data surveillance device” (數據監察器材) –

- (a) means any device or program used to monitor or record the input of

information into, or the output of information from, any information system by electronic means; but

(b) does not include an optical surveillance device;

“department” (部門) –

(a) in relation to interception (including any application for the issue or renewal of a prescribed authorization for interception, any prescribed authorization for interception and any other matter relating to interception), means a department specified in Part 1 of Schedule 1;

(b) in relation to covert surveillance (including any application for the issue or renewal of a prescribed authorization for covert surveillance, any prescribed authorization for covert surveillance and any other matter relating to covert surveillance), means a department specified in Part 2 of Schedule 1; or

(c) in relation to any other matter provided for in this Ordinance, means a department specified in Part 1 or 2 of Schedule 1;

“device” (器材) includes any instrument, apparatus and equipment;

“device retrieval warrant” (器材取出手令) means a device retrieval warrant issued under section 33 (and, where the context requires, includes a device retrieval warrant to be issued under that section);

“directorate officer” (首長級人員) means an officer not below a rank equivalent to that of chief superintendent of police;

“emergency authorization” (緊急授權) means an emergency authorization issued under Division 4 of Part 3 (and, where the context requires, includes an emergency authorization to be issued under that Division);

“enhancement equipment” (增強設備), in relation to a device, means any equipment used to enhance a signal, image or other information obtained by the use of the device;

“examination” (審查) means an examination (including consideration of the application for the examination) carried out under Division 3 of Part 4 (and, where the context requires, includes such an examination to be carried out under that Division);

“~~executive~~ District Court authorization” (~~行政~~區域法院授權) means an ~~executive~~ authorization issued or renewed by a judge of the District Court under Division 3 of Part 3 (and, where the context requires, includes an ~~executive~~ authorization to be issued or renewed by a judge of the District Court under that Division);

“function” (職能) includes power and duty;

“head” (首長), in relation to a department, includes any deputy ~~of the~~ head of the department;

“information system” (資訊系統) has the meaning assigned to it by section 2(1) of the Electronic Transactions Ordinance (Cap. 553);

“inspect” (查察) includes listen to, monitor and record;

“install” (裝設) includes attach;

“intercepting act” (截取作為), in relation to any communication, means the inspection of some or all of the contents of the communication, ~~in the course of its transmission by a postal service or by a telecommunications system,~~

- (i) by a person other than its sender or intended recipient or
- (ii) by a recipient who is an undercover agent or by any person on the instruction of or under the control of or with the cooperation of an officer of a department specified in Schedule 1;

“interception” (截取) –

- (a) in relation to any communication, means the carrying out of any intercepting act in respect of ~~the~~ that communication; or
- (b) when appearing in a context with no specific reference to any communication, means the carrying out of any intercepting act in respect of any communications;

“interception product” (截取成果) means any contents of a communication that have been obtained pursuant to ~~a prescribed authorization for~~ an interception, and includes a copy of such contents;

“journalistic content” (新聞內容) means any content of journalistic material;

“journalistic material” (新聞材料) has the meaning assigned to it by section 82 of the Interpretation and General Clauses Ordinance (Cap. 1);

~~“judicial judge’s Court of First Instance”~~ authorization” (司法法官原訟法庭授權) means a ~~judicial judge’s~~ an authorization issued or renewed by a judge of the Court of First Instance under Division 2 of Part 3 (and, where the context requires, includes a ~~judicial judge’s~~ an authorization to be issued or renewed by a judge of the Court of First Instance under that Division);

“listening device” (監聽器材) –

- (a) means any device used to overhear, listen to, monitor or record any conversation or words spoken to or by any person in conversation; but
- (b) does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment;

“maintain” (維修), in relation to a device, includes –

- (a) adjust, ~~relocate~~ reposition, repair or service the device; and
- (b) replace the device when it is faulty;

“optical surveillance device” (視光監察器材) –

- (a) means any device used to record visually or observe any activity; but
- (b) does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome the impairment;

“oral application” (口頭申請) means an oral application made under section ~~25(1)~~ 20(3);

~~“panel judge” (小組法官) means a judge appointed under section 6(1) to be a panel judge;~~

“postal article” (郵遞品) has the meaning assigned to it by section 2(1) of the

Post Office Ordinance (Cap. 98);

“postal interception” (郵件截取) means interception of any communication transmitted by a postal service;

“postal service” (郵政服務) means postal service ~~within the meaning of to~~ which the Post Office Ordinance (Cap. 98) applies;

“premises” (處所) includes any place and, in particular, includes –

- (a) any land or building;
- (b) any conveyance;
- (c) any structure (whether or not movable or offshore); and
- (d) any part of any of the premises described in paragraph (a), (b) or (c);

“prescribed authorization” (訂明授權) means a ~~judicial judge’s~~ Court of First Instance authorization, ~~an executive~~ a District Court authorization or an emergency authorization;

“Privacy Commissioner for Personal Data” (個人資料私隱專員) means the Commissioner as defined in the Personal Data (Privacy) Ordinance (Cap. 486) ;

“protected product” (受保護成果) means any interception product or surveillance product;

“public place” (公眾地方) –

- (a) means any premises which are a public place as defined in section 2(1) of the Summary Offences Ordinance (Cap. 228); but
- (b) does not include any such premises ~~to the extent~~ that ~~they~~ are intended for use by members of the public as a lavatory or as a place for taking a bath or changing clothes;

“public security” (公共安全) means the public security of Hong Kong, but does not include economic security;

“relevant authority” (有關當局) –

- (a) in relation to an application for the issue or renewal of a ~~Judicial judge’s~~ Court of First Instance authorization, means the ~~panel~~ judge of the Court of First Instance to whom the application is or has been made;
- (b) in relation to an application for the issue or renewal of ~~an executive~~ a District Court authorization, means the ~~authorizing officer~~ judge of the District Court to whom the application is or has been made; or
- (c) in relation to an application for the issue of an emergency authorization, means the head of a department to whom the application is or has been made;

“relevant purpose” (有關目的), in relation to a prescribed authorization, means the purpose sought to be furthered by carrying out the interception or covert surveillance concerned as described in section 3 for the purpose of the issue or renewal, or the continuance, of the prescribed authorization;

“relevant requirement” (有關規定) means any applicable requirement under –

- (a) any provision of this Ordinance;

- (b) the code of practice; or
- (c) any prescribed authorization or device retrieval warrant concerned;

“serious crime” (嚴重罪行) means any offence punishable –

- (a) in relation to the issue or renewal, or the continuance, of a prescribed authorization for interception, by a maximum penalty that is or includes a term of imprisonment of not less than 7 years; or
- (b) in relation to the issue or renewal, or the continuance, of a prescribed authorization for covert surveillance, by a maximum penalty that is or includes –
 - (i) a term of imprisonment of not less than ~~3~~ 7 years; ~~or~~
 - ~~(ii) a fine of not less than \$1,000,000;~~

“surveillance device” (監察器材) means –

- (a) a data surveillance device, a listening device, an optical surveillance device or a tracking device;
- (b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a); or
- (c) a device of a class prescribed by regulation made under section 62 for the purposes of this definition;

“surveillance product” (監察成果) means any material obtained pursuant to a prescribed authorization for covert surveillance, and includes a copy of the material;

“telecommunications interception” (電訊截取) means interception of any communication transmitted by a telecommunications system;

“telecommunications service” (電訊服務) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

“telecommunications system” (電訊系統) has the meaning assigned to it by section 2(1) of the Telecommunications Ordinance (Cap. 106);

“tracking device” (追蹤器材) means any electronic device used to determine or monitor the location of any person or any object or the status of any object;

~~“transmitted” (傳送) includes being transmitted;~~

“Type 1 surveillance” (第1 類監察) means any covert surveillance other than Type 2 surveillance;

“Type 2 surveillance” (第2 類監察), subject to subsections (3) and (3A), means any covert surveillance ~~to the extent~~ that –

- ~~(a) it is carried out with the use of a surveillance device for any purpose involving listening to, monitoring or recording words spoken or activity carried out by any person, and the person using the device is one –~~
 - ~~(i) who –~~
 - ~~(A) is the person speaking or carrying out the words or activity; or~~
 - ~~(B) is a person, or is included in a class of persons, by whom the~~

~~person described in sub-subparagraph (A) intends, or should reasonably expect, the words or activity to be heard or seen; or~~

~~(ii) who listens to, monitors or records the words or activity with the consent, express or implied, of a person described in subparagraph (i)(A) or (B); or~~

~~(a) is carried out with the use of a listening device or an optical surveillance device by any person for the purpose of listening to, monitoring or recording words spoken or activity carried out by any other person, if the person using the device—~~

~~(i) is a person by whom the other person intends, or should reasonably expect, the words or activity to be heard or seen; or~~

~~(ii) listens to, monitors or records the words or activity with the consent, express or implied, of a person described in subparagraph (i); or~~

~~(b) it is carried out with the use of an optical surveillance device or a tracking device and, if the use of the device does not involve —~~

~~(i) entry onto any premises either physically or by electronic means without permission; or~~

~~(ii) interference with the interior of any conveyance or object without permission.~~

~~(2) For the purposes of this Ordinance, a person is not regarded as being entitled to a reasonable expectation of privacy within the meaning of paragraph (a)(i) of the definition of “covert surveillance” in subsection (1) in relation to any activity carried out by him in a public place, but nothing in this subsection affects any such entitlement of the person in relation to words spoken, written or read by him in a public place.~~

(3) For the purposes of this Ordinance, any covert surveillance which is Type 2 surveillance under the definition of “Type 2 surveillance” in subsection (1) is regarded as Type 1 surveillance if it is likely that any information which may be subject to legal professional privilege will be obtained by carrying it out.

(3A) An officer of a department may apply for the issue or renewal of a prescribed authorization for any Type 2 surveillance as if the Type 2 surveillance were Type 1 surveillance, and the provisions of this Ordinance relating to the application and the prescribed authorization apply to the Type 2 surveillance as if it were Type 1 surveillance.

~~(4) For the purposes of this Ordinance—~~

~~(a) a communication transmitted by a postal service is regarded as being in the course of the transmission if it is regarded as being in course of transmission by post under section 2(2) of the Post Office Ordinance (Cap. 98); and~~

~~(b) a communication transmitted by a telecommunications system is not~~

~~regarded as being in the course of the transmission if it has been received by the intended recipient of the communication or by an information system or facility under his control or to which he may have access, whether or not he has actually read or listened to the contents of the communication.~~

- (5) For the purposes of this Ordinance, the contents of any communication transmitted by a telecommunications system include any data produced in association with the communication.

(5A) For the purposes of this Ordinance, *association, assembly, strike, confrontation, advocacy, protest or dissent (whether in furtherance of a political or social objective or otherwise), unless likely intended to be carried on by violent means, is not of itself regarded as a threat to public security.*

(5B) For the purposes of this Ordinance, any act prescribed under Article 23 of the Basic Law, unless intended to be carried on by violent means (more than negligible), is not of itself regarded as a threat to public security.

- (6) For the purposes of this Ordinance –

- (a) an application is ~~also~~ regarded as being made orally if it is made orally in person or made by telephone, video conferencing or other electronic means by which words spoken can be heard (whether or not any part of the application is made in writing);
- (b) information is ~~also~~ regarded as being provided orally if it is provided orally in person or provided by telephone, video conferencing or other electronic means by which words spoken can be heard (whether or not any part of the information is provided in writing); and
- (c) a determination (including the issue of a prescribed authorization or a renewed prescribed authorization and the giving of any reason) is ~~also~~ regarded as being delivered orally if it is delivered orally in person or delivered by telephone, video conferencing or other electronic means by which words spoken can be heard (whether or not any part of the determination is delivered in writing).

~~(7) Without prejudice to section 54 of the Interpretation and General Clauses Ordinance (Cap. 1), any reference in this Ordinance to a panel judge or any officer of a department (however expressed) includes –~~

- ~~(a) where the person who has been such panel judge or officer is no longer holding office as such panel judge or officer, the person for the time being holding such office or appointed to act in or perform the functions of such office or lawfully performing the functions of such office; or~~
- ~~(b) where the person who is such panel judge or officer is unable to perform the functions of the office of such panel judge or officer, the person for the time being appointed to act in or perform the functions of such office or lawfully performing the functions of such office.~~

3. Conditions for issue, renewal or continuance of prescribed authorization

- (1) In this Ordinance, the conditions for the issue or renewal, or the continuance, of a prescribed authorization, are that, in the circumstances of the particular case –
- (a) the purpose sought to be furthered by carrying out the interception or covert surveillance concerned is that of –
 - (i) preventing or detecting serious crime; or
 - (ii) protecting public security; ~~and~~
 - (aa) there is reasonable suspicion that any person has been, is, or is likely to be, involved in –
 - (i) where the purpose sought to be furthered by carrying out the interception or covert surveillance is that specified in paragraph (a)(i), the particular serious crime to be prevented or detected; or
 - (ii) where the purpose sought to be furthered by carrying out the interception or covert surveillance is that specified in paragraph (a)(ii), any activity which constitutes or would constitute the particular *imminent* threat to public security; and
 - (b) the interception or covert surveillance is necessary for, and proportionate to, the purpose sought to be furthered by carrying it out, upon –
 - (i) balancing, ~~in operational terms,~~ the relevant factors against the intrusiveness of the interception or covert surveillance on any person who is to be the subject of or may be affected by the interception or covert surveillance; ~~and~~
 - (ii) considering whether the purpose sought to be furthered by carrying out the interception or covert surveillance can reasonably be furthered by other less intrusive means; ~~and~~
 - (iii) ~~considering such other matters~~ *whether the issue or renewal or the continuance of a prescribed authorization can be justified in view of human rights factors, including –*
 - (A) *the right to freedom and privacy protected by Article 30 of the Basic Law; and*
 - (B) *the rights and freedoms protected in the Basic Law and the International Covenant on Civil and Political Rights*
- ~~that are relevant in the circumstances.~~
- (2) In this section, “relevant factors” (有關因素) means –
- (a) the immediacy and gravity of –
 - (i) where the purpose sought to be furthered by carrying out the interception or covert surveillance concerned is that specified in subsection (1)(a)(i), the particular serious crime to be prevented or detected; or
 - (ii) where the purpose sought to be furthered by carrying out the interception or covert surveillance concerned is that specified in

- subsection (1)(a)(ii), the particular threat to public security; and
- (b) the likely value and relevance, in relation to the purpose sought to be furthered by carrying out the interception or covert surveillance, of the information likely to be obtained by carrying it out.

PART 2

PROHIBITION ON INTERCEPTION AND COVERT SURVEILLANCE

4. Prohibition on interception

(1) Subject to subsection (2), ~~no~~ *Neither the Chief Executive, bureau heads insofar as they are not public servants nor any* public officer shall, directly or indirectly (whether through any other person or otherwise), carry out any interception in his public capacity.

(1A) Contravention to subsection (1) shall be an offence punishable with a maximum penalty of 2 years imprisonment.

(2) Subsection (1) does not apply to –

- (a) any interception carried out pursuant to a prescribed authorization;
- (b) any interception of telecommunications transmitted by radiocommunications (other than the radiocommunications part of a telecommunications network for the provision of a public telecommunications service by any carrier licensee under the Telecommunications Ordinance (Cap. 106)); and
- (c) any interception authorized, permitted or required to be carried out by or under any enactment other than this Ordinance (including any interception carried out in the course of the execution of an order of a court authorizing the search of any premises or the seizure of any evidence).

(3) In this section, “carrier licensee” (傳送者牌照持有人), “public telecommunications service” (公共電訊服務), “radiocommunications” (無線電通訊), “telecommunications” (電訊) and “telecommunications network” (電訊網絡) have the meanings respectively assigned to them by section 2(1) of the Telecommunications Ordinance (Cap. 106)._____.

5. Prohibition on covert surveillance

(1) Subject to subsection (2), ~~no~~ *Neither the Chief Executive, bureau heads insofar as they are not public servants nor any* public officer shall, directly or indirectly (whether through any other person or otherwise), carry out any covert surveillance in his public capacity.

(1A) Contravention to subsection (1) shall be an offence punishable with a maximum penalty of 2 years imprisonment.

(2) Subsection (1) does not apply to any covert surveillance carried out pursuant to a prescribed authorization.

PART 3
PRESCRIBED AUTHORIZATIONS, ETC.
Division 1 – Relevant Authorities

6. Panel judges

- ~~(1) The Chief Executive shall, on the recommendation of the Chief Justice, appoint 3 to 6 eligible judges to be panel judges for the purposes of this Ordinance.~~
- ~~(2) A panel judge shall be appointed for a period of 3 years, and may from time to time be reappointed.~~
- ~~(3) The Chief Executive may, on the recommendation of the Chief Justice, revoke the appointment of a panel judge for good cause.~~
- ~~(3A) In performing any of his functions under this Ordinance, a panel judge—~~
- ~~(a) is not regarded as a court or a member of a court; but~~
- ~~(b) has the same powers, protection and immunities as a judge of the Court of First Instance has in relation to proceedings in that Court.~~
- ~~(4) Schedule 2 applies to and in relation to the procedures of, and other matters relating to, a panel judge.~~
- ~~(4A) A person previously appointed as a panel judge may from time to time be further appointed as such in accordance with the provisions of this Ordinance that apply to the appointment of a panel judge.~~
- ~~(5) In this section, “eligible judge” (合資格法官) means a judge of the Court of First Instance.~~

6. Judges

- (1) For the purposes of this Ordinance, a judge refers either a judge of the Court of First Instance or a judge of the District Court.
- (2) Schedule 2 applies to and in relation to the procedures of, and other matters relating to, a judge.

7. Authorizing officers

~~The head of a department may designate any officer not below a rank equivalent to that of senior superintendent of police to be an authorizing officer for the purposes of this Ordinance.~~

Division 2 – Judicial Judge’s Court of First Instance Authorizations
Issue of judicial judge’s Court of First Instance authorizations

8. Application for judicial judge’s Court of First Instance authorization for interception or Type 1 surveillance

- (1) An officer of a department may apply to a ~~panel judge~~ a judge of the Court of First Instance for the issue of a ~~judicial judge's~~ an authorization for any interception or Type 1 surveillance to be carried out by or on behalf of any of the officers of the department.
- (2) The application is –
- (aa) to be made ex parte;
- (a) to be made in writing; and
- (b) to be supported by an affidavit of the applicant which is to comply with the requirements specified in –
- (i) in the case of a ~~judicial judge's~~ an authorization for interception, Part 1 of Schedule 3; or
- (ii) in the case of a ~~judicial judge's~~ an authorization for Type 1 surveillance, Part 2 of Schedule 3.
- (3) An application may not be made under subsection (1) unless the making of the application has been approved by a directorate officer of the department concerned.

9. Determination of application for ~~judicial judge's~~ Court of First Instance authorization

- (1) Upon considering an application for the issue of a ~~judicial judge's~~ an authorization made under section 8, the ~~panel judge~~ of the Court of First Instance may, subject to subsection (2) –
- (a) issue the ~~judicial judge's~~ authorization sought under the application, with or without variations; or
- (b) refuse to issue the ~~judicial judge's~~ authorization.
- (1A) When considering the application in subsection (1), the judge of the Court of First Instance may invite the Privacy Commissioner for Personal Data to make submission as a special advocate in camera.
- (2) The ~~panel judge~~ of the Court of First Instance shall not issue the ~~judicial judge's~~ authorization unless he is satisfied that the conditions for its issue under section 3 have been met.
- (3) The ~~panel judge~~ of the Court of First Instance shall deliver his determination under subsection (1) by –
- (a) in the case of subsection (1)(a), issuing the ~~judicial judge's~~ authorization in writing with reason; or
- (b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

10. Duration of ~~judicial judge's~~ Court of First Instance authorization

- ~~A judicial judge's~~ An authorization –
- (a) takes effect at the time specified by the ~~panel judge~~ of the Court of First Instance when issuing the ~~judicial judge's~~ authorization, which in any case is not to be earlier than the time when it is issued; and

- (b) subject to any renewal under this Division, ceases to have effect upon the expiration of the period specified by the ~~panel judge~~ of Court of First Instance when issuing the ~~judicial judge's~~ authorization, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Renewal of ~~judicial judge's~~ Court of First Instance authorizations

11. Application for renewal of ~~judicial judge's~~ Court of First Instance authorization

(1) ~~At any time before a judicial judge's an~~ authorization ceases to have effect, an officer of the department concerned may apply to a ~~panel judge~~ of the Court of First Instance for the renewal of the ~~judicial judge's~~ authorization.

(2) ~~The application is –~~

(aa) to be made ex parte;

(a) ~~to be made in writing; and~~

(b) ~~to be supported by –~~

(i) a copy of the ~~judicial judge's~~ authorization sought to be renewed;

(ii) ~~a copy of any affidavit~~ copies of all affidavits provided under this

Part for the purposes of any application for the issue or renewal of the ~~judicial judge's~~ authorization, or for the purposes of any application made further to an oral application for confirmation of the ~~judicial judge's~~ authorization or its previous renewal; and

(iii) an affidavit of the applicant which is to comply with the requirements specified in Part 4 of Schedule 3.

(3) An application may not be made under subsection (1) unless the making of the application has been approved by a directorate officer of the department concerned.

12. Determination of application for renewal of ~~judicial judge's~~ Court of First Instance authorization

(1) Upon considering an application for the renewal of ~~a judicial judge's an~~ authorization made under section 11, the ~~panel judge~~ of the Court of First Instance may, subject to subsection (2) –

(a) grant the renewal sought under the application, with or without variations;
or

(b) refuse to grant the renewal.

(1A) When considering the application in subsection (1), the judge of the Court of First Instance may invite the Privacy Commissioner for Personal Data to make submission as a special advocate in camera.

(1B) When consider the application in subsection (1), the judge of the Court of First Instance shall take into account the total duration of the authorization.

(2) The ~~panel judge~~ of the Court of First Instance shall not grant the renewal

unless he is satisfied that the conditions for ~~its grant the renewal~~ under section 3 have been met.

(3) The ~~panel~~ judge of the Court of First Instance shall deliver his determination under subsection (1) by –

- (a) in the case of subsection (1)(a), issuing the renewed ~~judicial judge's~~ authorization in writing with reason; or
- (b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

(4) ~~A judicial judge's~~ An authorization may be renewed more than once under this Ordinance.

13. Duration of renewal of ~~judicial judge's Court of First Instance~~ authorization

A renewal of ~~a judicial judge's~~ an authorization –

- (a) takes effect at the time when the ~~judicial judge's~~ authorization would have ceased to have effect but for the renewal; and
- (b) subject to any further renewal under this Division, ceases to have effect upon the expiration of the period specified by the ~~panel~~ judge of the Court of First Instance when granting the renewal, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Division 3 – ~~Executive~~ District Court Authorizations ***Issue of ~~executive~~ District Court authorizations***

14. Application for ~~executive District Court~~ authorization for Type 2 surveillance

(1) An officer of a department may apply to ~~an authorizing officer of the department~~ a judge of the District Court for the issue of an ~~executive~~ authorization for any Type 2 surveillance to be carried out by or on behalf of any of the officers of the department.

(2) The application is –

(aa) to be made ex parte;

- (a) to be made in writing; and
- (b) to be supported by ~~a statement in writing made by~~ an affidavit of the applicant which is to comply with the requirements specified in Part 3 of Schedule 3.

15. Determination of application for ~~executive District Court~~ authorization

(1) Upon considering an application for the issue of an ~~executive~~ authorization made under section 14, the ~~authorizing officer~~ judge of the District Court may, subject to subsection (2) –

- (a) issue the ~~executive~~ authorization sought under the application, with or without variations; or
- (b) refuse to issue the ~~executive~~ authorization.

(1A) When considering the application in subsection (1), the judge of the District Court may invite the Privacy Commissioner for Personal Data to make submission as a special advocate in camera.

(2) The ~~authorizing officer~~ judge of the District Court shall not issue the ~~executive~~ authorization unless he is satisfied that the conditions for its issue under section 3 have been met.

(3) The ~~authorizing officer~~ judge of the District Court shall deliver his determination under subsection (1) by –

- (a) in the case of subsection (1)(a), issuing the ~~executive~~ authorization in writing with reason; or
- (b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

16. Duration of ~~executive~~ District Court authorization

An ~~executive~~ authorization –

- (a) takes effect at the time specified by the ~~authorizing officer~~ judge of the District Court when issuing the ~~executive~~ authorization, which in any case is not to be earlier than the time when it is issued; and
- (b) subject to any renewal under this Division, ceases to have effect upon the expiration of the period specified by the ~~authorizing officer~~ judge of the District Court when issuing the ~~executive~~ authorization, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Renewal of ~~executive~~ District Court authorizations

17. Application for renewal of ~~executive~~ District Court authorization

(1) At any time before an ~~executive~~ authorization ceases to have effect, an officer of the department concerned may apply to ~~authorizing officer of the department a~~ judge of the District Court for the renewal of the ~~executive~~ authorization.

(2) The application is –

(aa) to be made ex parte;

(a) to be made in writing; and

(b) to be supported by –

- (i) a copy of the ~~executive~~ authorization sought to be renewed;
- (ii) ~~a copy of any statement~~ copies of all statements affidavits provided under this Part for the purposes of any application for the issue or renewal of the ~~executive~~ authorization, or for the purposes of any application made further to an oral application for confirmation of the ~~executive~~ authorization or its previous renewal; and
- (iii) ~~a statement in writing made by~~ an affidavit of the applicant which is to comply with the requirements specified in Part 4 of Schedule 3.

18. Determination of application for renewal of executive District Court authorization

(1) Upon considering an application for the renewal of an ~~executive~~ authorization made under section 17, the ~~authorizing officer~~ *judge of the District Court* may, subject to subsection (2) –

(a) grant the renewal sought under the application, with or without variations; or

(b) refuse to grant the renewal.

(1A) When considering the application in subsection (1), the judge of the District Court may invite the Privacy Commissioner for Personal Data to make submission as a special advocate in camera.

(1B) When consider the application in subsection (1), the judge of the Court of First Instance shall take into account the total duration of the authorization.

(2) The ~~authorizing officer~~ *judge of the District Court* shall not grant the renewal unless he is satisfied that the conditions for ~~its grant~~ the renewal under section 3 have been met.

(3) The ~~authorizing officer~~ *judge of the District Court* shall deliver his determination under subsection (1) by –

(a) in the case of subsection (1)(a), issuing the renewed ~~executive~~ authorization in writing *with reason*; or

(b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

(4) An ~~executive~~ authorization may be renewed more than once under this Ordinance.

19. Duration of renewal of executive District Court authorization

A renewal of an ~~executive~~ authorization –

(a) takes effect at the time when the ~~executive~~ authorization would have ceased to have effect but for the renewal; and

(b) subject to any further renewal under this Division, ceases to have effect upon the expiration of the period specified by the ~~authorizing officer~~ *judge of the District Court* when granting the renewal, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

Division 4 – Emergency Authorizations *Issue of emergency authorizations*

20. Application for emergency authorization for interception or Type 1 surveillance in case of emergency

(1) An officer (*not less than the rank of superintendent of police or equivalent*) of a department may apply to the head of the department for the issue of an emergency authorization for any interception or Type 1 surveillance to be carried out by or on behalf of any of the officers of the department, if he considers that –

- (a) there is immediate need for the interception or Type 1 surveillance to be carried out by reason of an imminent risk of –
 - (i) death or serious bodily harm of any person;
 - (ii) substantial damage to property;
 - (iii) serious threat to public security; or
 - (iv) loss of vital evidence; and
- (b) having regard to all the circumstances of the case, it is not reasonably practicable to apply for the issue of a ~~judicial judge's~~ Court of First Instance authorization for the interception or Type 1 surveillance.

(2) The application is –

- (a) to be made in writing; and
- (b) to be supported by a statement in writing made by the applicant which is to –
 - (i) set out the reason for making the application; and
 - (ii) comply with –
 - (A) in the case of an emergency authorization for interception, the requirements specified in Part 1 of Schedule 3 which are to apply to the statement as they apply to an affidavit referred to in section 8(2)(b); or
 - (B) in the case of an emergency authorization for Type 1 surveillance, the requirements specified in Part 2 of Schedule 3 which are to apply to the statement as they apply to an affidavit referred to in section 8(2)(b).

(3) An application for emergency authorization under subsection (1) may be made orally in person if, having regard to all circumstances of the case, it is not reasonably practicable to make an application in writing.

(4) Where an oral application is made, the application shall make an oral statement providing the required information specified in Part 2 of Schedule 3 as the case may be.

21. Determination of application for emergency authorization

(1) Upon considering an application for the issue of an emergency authorization made under section 20, the head of the department concerned may, subject to subsection (2) –

- (a) issue the emergency authorization sought under the application, with or without variations; or
- (b) refuse to issue the emergency authorization.

(2) The head of the department shall not issue the emergency authorization unless he is satisfied –

- (a) that section 20(1)(a) and (b) applies; ~~and~~
- (aa) that, where an oral application is made, section 20(3) applies; and
- (b) that the conditions for the issue of the emergency authorization under section

3 have been met.

(3) The head of the department shall deliver his determination under subsection (1) by –

- (a) in the case of subsection (1)(a), issuing the emergency authorization in writing with reason; or
- (b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

22. Duration of emergency authorization

(1) An emergency authorization –

- (a) takes effect at the time specified by the head of the department concerned when issuing the emergency authorization, which in any case is not to be earlier than the time when it is issued; and
- (b) ceases to have effect upon the expiration of the period specified by the head of the department when issuing the emergency authorization, which in any case is not to be longer than the period of 48 hours beginning with the time when it takes effect.

(2) Without prejudice to any application under section 8 for the issue of any ~~judicial judge's~~ Court of First Instance authorization for the interception or Type 1 surveillance concerned, an emergency authorization may not be renewed under this Ordinance.

Application for confirmation of emergency authorizations

23. Application for confirmation of emergency authorization

(1) Where any interception or Type 1 surveillance is carried out pursuant to an emergency authorization, the head of the department concerned shall cause an officer of the department to apply to a ~~panel~~ judge of the Court of First Instance for confirmation of the emergency authorization, as soon as reasonably practicable after, and in any event within the period of 48 hours beginning with, the time when the emergency authorization takes effect.

(2) The application is –

(aa) to be made ex parte;

(a) to be made in writing; and

(b) to be supported by –

(i) a copy of the emergency authorization; and

(ii) an affidavit of the applicant which is to verify the contents of the statement provided under section 20(2)(b) for the purposes of the application for the issue of the emergency authorization.

(3) ~~If no~~ In default of any application being made for confirmation of the emergency authorization ~~is made~~ within the period of 48 hours referred to in subsection (1), the head of the department concerned shall –

- (a) cause the immediate destruction of any information obtained by carrying out the interception or Type 1 surveillance concerned, and any further

~~information or intelligence or record derived from such information to the extent that it could not have been obtained without carrying out the interception or Type 1 surveillance;~~ and

- (b) without prejudice to section 52, submit to the Commissioner a report with details of the case.

24. Determination of application for confirmation of emergency authorization

(1) Upon considering an application for confirmation of an emergency authorization as provided for in section 23(1), the ~~panel~~ judge of the Court of First Instance may, subject to subsection (2) –

- (a) confirm the emergency authorization; or
- (b) refuse to confirm the emergency authorization.

(1A) When considering the application in subsection (1), the judge of the Court of First Instance may invite the Privacy Commissioner for Personal Data to make submission as a special advocate in camera.

(2) The ~~panel~~ judge of the Court of First Instance shall not confirm the emergency authorization unless he is satisfied that section 21(2)(b) has been complied with in the issue of the emergency authorization. The judge of the Court of First Instance may invite the Commissioner of Privacy to assist him in arriving such conclusion.

(3) Where the ~~panel~~ judge of the Court of First Instance refuses to confirm the emergency authorization under subsection (1)(b), he may make one or more of the following orders –

- (a) in any case where the emergency authorization still has effect at the time of the determination, an order that the emergency authorization is, notwithstanding any other provision of this Ordinance –
 - (i) to be revoked upon the making of the determination; or
 - (ii) only to have effect subject to the variations specified by him, from the time of the determination;
- (b) in any case whether or not the emergency authorization still has effect at the time of the determination, an order that the head of the department concerned shall cause the immediate destruction of ~~any information obtained by carrying out the interception or Type 1 surveillance concerned, to the extent –~~
 - (i) subject to subparagraph (ii), ~~that it could not have been obtained without carrying out the interception or Type 1 surveillance~~ any information obtained by carrying out the interception or Type 1 surveillance concerned, and any further information or intelligence or record derived from such information; or
 - (ii) where paragraph (a)(ii) applies, any information obtained by carrying out the interception or Type 1 surveillance concerned that is specified in the order, and any further information or intelligence or record derived from such information.

(4) Where the emergency authorization is revoked under subsection (3)(a)(i), the emergency authorization is, notwithstanding section 22(1)(b), to cease to have effect from the time of the revocation.

(5) The panel judge of the Court of First Instance shall deliver his determination under subsection (1) by –

- (a) in the case of subsection (1)(a), endorsing his confirmation on the emergency authorization in writing with reason; or
- (b) in the case of subsection (1)(b), giving the reason for the refusal and making any order under subsection (3) in writing.

~~Division 5 – Special Provisions for Oral Applications~~ ~~Oral applications~~

~~25. Oral application and its effect~~

~~(1) Notwithstanding the relevant written application provision, an application for the issue or renewal of a prescribed authorization under this Ordinance may be made orally, if the applicant considers that, having regard to all the circumstances of the case, it is not reasonably practicable to make the application in accordance with the relevant written application provision.~~

~~(2) Notwithstanding the relevant determination provision and without prejudice to the relevant conditions provision, where an oral application is made, the relevant authority shall not issue or grant the prescribed authorization or renewal sought under the application unless he is satisfied that, having regard to all the circumstances of the case, it is not reasonably practicable to make the application in accordance with the relevant written application provision.~~

~~(3) Notwithstanding the relevant document provision, where an oral application is made, the information required to be provided for the purposes of the application under the relevant document provision may be provided orally (and accordingly any requirement as to the making of any affidavit or statement does not apply).~~

~~(4) Notwithstanding the relevant written determination provision, where an oral application is made, the relevant authority may deliver the determination required to be delivered in respect of the application under the relevant determination provision by –~~

~~(a) issuing the prescribed authorization or the renewed prescribed authorization orally; or~~

~~(b) where he refuses to issue or grant the prescribed authorization or renewal sought under the application, giving the reason for the refusal orally.~~

~~(5) Except as otherwise provided in this Division, any oral application and any prescribed authorization or renewal issued or granted as a result of that application are for all purposes regarded as having the same effect respectively as an application made in writing and a prescribed authorization or renewal issued or granted as a result of that application, and the provisions of this Ordinance are, subject to necessary modifications, to apply accordingly.~~

~~(6) In this section—~~

~~“relevant conditions provision” (有關條件條文) means section 9(2), 12(2), 15(2), 18(2) or 21(2) (as may be applicable);~~

~~“relevant determination provision” (有關決定條文) means section 9(1), 12(1), 15(1), 18(1) or 21(1) (as may be applicable);~~

~~“relevant document provision” (有關文件條文) means section 8(2)(b), 11(2)(b), 14(2)(b), 17(2)(b) or 20(2)(b) (as may be applicable);~~

~~“relevant written application provision” (有關書面申請條文) means section 8(2)(a), 11(2)(a), 14(2)(a), 17(2)(a) or 20(2)(a) (as may be applicable);~~

~~“relevant written determination provision” (有關書面決定條文) means section 9(3), 12(3), 15(3), 18(3) or 21(3) (as may be applicable).~~

~~***Application for confirmation of prescribed authorizations or renewals issued or granted upon oral applications***~~

~~26. Application for confirmation of prescribed authorization or renewal issued or granted upon oral application~~

~~(1) Where, as a result of an oral application, the prescribed authorization or renewal sought under the application has been issued or granted, the head of the department concerned shall cause an officer of the department to apply to the relevant authority for confirmation of the prescribed authorization or renewal, as soon as reasonably practicable after, and in any event within the period of 48 hours beginning with, the time when the prescribed authorization or renewal takes effect.~~

~~(2) The application is—~~

~~(a) to be made in writing; and~~

~~(b) to be supported by—~~

~~(i) a record in writing containing all the information that would have been provided to the relevant authority in writing under the relevant written application provision had the oral application been made in writing;~~

~~(ii) where section 25(3) applies in relation to the oral application—~~

~~(A) where the relevant authority is a panel judge, an affidavit of the applicant which is to verify all the information provided pursuant to that section for the purposes of the oral application; or~~

~~(B) where the relevant authority is not a panel judge, a statement in writing made by the applicant setting out all the information provided pursuant to that section for the purposes of the oral application; and~~

~~(iii) where section 25(4) applies in relation to the oral application, a record in writing setting out the determination delivered pursuant to that section in respect of the oral application.~~

~~(3) If no In default of any application being made for confirmation of the prescribed authorization or renewal is made within the period of 48 hours referred to in subsection (1), then—~~

~~(a) in any case where the prescribed authorization or renewal still has effect upon the expiration of the period, the prescribed authorization or renewal is, notwithstanding any other provision of this Ordinance, to be regarded as revoked upon the expiration of the period; and~~

~~(b) in any case whether or not the prescribed authorization or renewal still has effect upon the expiration of the period, the head of the department concerned shall—~~

~~(i) cause the immediate destruction of any information obtained by carrying out the interception or covert surveillance concerned, to the extent that it could not have been obtained without carrying out the interception or covert surveillance; and~~

~~(ii) without prejudice to section 52, submit to the Commissioner a report with details of the case.—~~

~~(4) Where the prescribed authorization or renewal is regarded as revoked under subsection (3)(a), the prescribed authorization or renewal is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.~~

(4A) If, at the time of an application for confirmation of the prescribed authorization or renewal as provided for in subsection (1), the relevant authority is no longer holding his office or performing the relevant functions of his office—

(a) without prejudice to section 54 of the Interpretation and General Clauses Ordinance (Cap. 1), the reference to relevant authority in that subsection includes the person for the time being appointed as a panel judge or authorizing officer (as the case may be) and lawfully performing the relevant functions of the office of that relevant authority; and

(b) the provisions of this section and section 27 are to apply accordingly.

~~(5) In this section—~~

~~“relevant duration provision” (有關時限條文) means section 10(b), 13(b), 16(b) or 19(b) (as may be applicable);~~

~~“relevant written application provision” (有關書面申請條文) means section 8(2)(a), 11(2)(a), 14(2)(a), 17(2)(a) or 20(2)(a) (as may be applicable).~~

27. Determination of application for confirmation of prescribed authorization or renewal issued or granted upon oral application

~~(1) Upon considering an application for confirmation of a prescribed authorization or renewal as provided for in section 26(1), the relevant authority may, subject to subsection (2)—~~

~~(a) confirm the prescribed authorization or renewal; or~~

~~(b) refuse to confirm the prescribed authorization or renewal.~~

~~(2) The relevant authority shall not confirm the prescribed authorization or renewal unless he is satisfied that the relevant conditions~~

~~provision has been complied with in the issue or grant of the prescribed authorization or renewal.~~

~~(3) Where the relevant authority refuses to confirm the prescribed authorization or renewal under subsection (1)(b), he may make one or more of the following orders—~~

~~(a) in any case where the prescribed authorization or renewal still has effect at the time of the determination, an order that the prescribed authorization or renewal is, notwithstanding any other provision of this Ordinance—~~

~~(i) to be revoked upon the making of the determination; or~~

~~(ii) only to have effect subject to the variations specified by him, from the time of the determination;~~

~~(b) in any case whether or not the prescribed authorization or renewal still has effect at the time of the determination, an order that the head of the department concerned shall cause the immediate destruction of any information obtained by carrying out the interception or covert surveillance concerned, to the extent—~~

~~(i) subject to subparagraph (ii), that it could not have been obtained without carrying out the interception or covert surveillance any information obtained by carrying out the interception or covert surveillance concerned; or~~

~~(ii) where paragraph (a)(ii) applies, any information obtained by carrying out the interception or covert surveillance concerned that is specified in the order.~~

~~(4) Where the prescribed authorization or renewal is revoked under subsection (3)(a)(i), the prescribed authorization or renewal is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.~~

~~(5) The relevant authority shall deliver his determination under subsection (1) by—~~

~~(a) in the case of subsection (1)(a), issuing the prescribed authorization or the renewed prescribed authorization (being the prescribed authorization confirmed under that subsection or being in terms of the renewal confirmed under that subsection (as the case may be)) in writing; or~~

~~(b) in the case of subsection (1)(b), giving the reason for the refusal and making any order under subsection (3) in writing.~~

~~(6) In this section—~~

~~“relevant conditions provision” (有關條件條文) means section 9(2), 12(2), 15(2), 18(2) or 21(2)(b) (as may be applicable);~~

~~“relevant duration provision” (有關時限條文) means section 10(b), 13(b), 16(b), 19(b) or 22(1)(b) (as may be applicable).~~

~~28. Special case of emergency authorization issued as a result of oral application~~

~~(1) Where an emergency authorization is issued as a result of an oral application, sections 26 and 27 do not apply if—~~

~~(a) an application for confirmation of the emergency authorization as provided for in section 23(1) has been made to a panel judge within the period of 48 hours referred to in that section; and~~

~~(b) the application is supported by—~~

~~(i) a record referred to in section 26(2)(b)(i);~~

~~(ii) an affidavit of the applicant which is to verify the contents of the statement provided under section 20(2)(b) for the purposes of the application for the issue of the emergency authorization or, where section 25(3) applies in relation to the oral application, all the information provided pursuant to section 25(3) for the purposes of the oral application; and~~

~~(iii) a copy of the emergency authorization or, where section 25(4) applies in relation to the oral application, a record in writing setting out the determination delivered pursuant to that section in respect of the oral application.~~

~~(2) Notwithstanding section 23(2)(b), the application described in subsection (1)(a) and (b) is for all purposes regarded as an application duly made for confirmation of the emergency authorization as provided for in section 23(1), and the provisions of this Ordinance are to apply accordingly (subject to section 24(5)(a) being read as requiring the panel judge to deliver his determination under section 24(1) by issuing the emergency authorization (being the emergency authorization confirmed under section 24(1)(a)) in writing).~~

Division 6 – General Provisions for Prescribed Authorizations *Matters authorized, required or provided for by prescribed authorizations*

29. What a prescribed authorization may authorize or require under or by virtue of its terms, etc.

- (1) A prescribed authorization for interception may –
 - (a) in the case of a postal interception, contain terms that authorize one or both of the following –
 - (i) the interception of communications made to or from any premises or address specified in the prescribed authorization;
 - (ii) the interception of communications made to or by any person specified in the prescribed authorization (whether by name or by description); or
 - (b) in the case of a telecommunications interception, contain terms that authorize one or both of the following –
 - (i) the interception of communications made to or from any telecommunications service specified in the prescribed authorization;
 - (ii) the interception of communications made to or from any telecommunications service that any person specified in the prescribed authorization (whether by name or by description) is using, or is ~~likely~~ **reasonably expected** to use.
- (2) A prescribed authorization for covert surveillance may contain terms that authorize one or more of the following –
 - (a) the use of any surveillance devices in or on any premises specified in the prescribed authorization;
 - (b) the use of any surveillance devices in or on any object or class of objects specified in the prescribed authorization;
 - (c) the use of any surveillance devices in respect of the conversations, activities or location of any person specified in the prescribed authorization (whether by name or by description).
- (3) A prescribed authorization, ~~other than an executive authorization,~~ may contain terms that authorize the doing of anything reasonably necessary to conceal any conduct authorized or required to be carried out under the prescribed authorization, **provided that an assessment of the risk and damage arising from the concealment has been submitted before the determination of the authorization and that the nature of concealment so authorized must be specified in the authorization.**
- (4) A prescribed authorization, ~~other than an executive authorization,~~ may, if it is **reasonably** necessary for the execution of the prescribed authorization, contain terms that authorize the interference with any property (whether or not of any person who is the subject of the interception or covert surveillance concerned) **provided that an assessment of the risk and damage arising from the interference with any property has been submitted before the determination of the authorization and that the nature of interference so authorized must be specified in the authorization.**

- (5) A prescribed authorization, ~~other than an executive authorization,~~ may contain terms that require any person specified in the prescribed authorization (whether by name or by description), on being shown a copy of the prescribed authorization, to provide to any of the officers of the department concerned such reasonable assistance for the execution of the prescribed authorization as is specified in the prescribed authorization. provided that –
- (i) an assessment of the implication of assistance has been submitted before the determination of the authorization;
 - (ii) the nature of assistance so authorized must be specified in the authorization; and
 - (iii) no authorization shall require the specified person to incur any expense.
- (6) A prescribed authorization for interception ~~also~~ may contain terms that authorize ~~authorizes~~ –
- (a) the installation, use and maintenance of any devices required to be used in order to intercept any of the communications authorized to be intercepted under the prescribed authorization provided that if the device is to be installed or used in any private property,
 - (i) an assessment of the risk and damage arising from the installation and use of such device has been submitted before the determination of the authorization; and
 - (ii) the address and if ascertainable, the owner, tenant and occupier of such property must be specified in the authorization;
 - (b) the entry, by the use of reasonable force if necessary, onto any premises in order to carry out any conduct authorized or required to be carried out under the prescribed authorization provided that an assessment of the risk and damage arising from the entry has been submitted before the determination of the authorization;
- (6A) A prescribed authorization for interception also authorizes –
- ~~(a)~~ (a) the incidental interception of any communication which ~~it is necessary to intercept in order to intercept necessarily arises from the interception of any of the~~ communications authorized to be ~~intercepted~~ carried out under the prescribed authorization; and
 - ~~(b)~~ (b) where subsection (1)(a)(ii) or (b)(ii) is applicable, the provision to any person, for the execution of the prescribed authorization, of particulars of the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying –
 - (i) in the case of subsection (1)(a)(ii), the communications made to or by the person specified in the prescribed authorization; or
 - (ii) in the case of subsection (1)(b)(ii), the communications made to or from any telecommunications service that the person specified in the prescribed authorization is using, or is likely to use.

- (7) A prescribed authorization for covert surveillance ~~also~~ may contain terms that authorize ~~authorizes~~ –
- (a) where subsection (2)(a) is applicable –
- (i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization in or on the premises specified in the prescribed authorization provided that if the surveillance device is to be installed or used in any private property –
- (A) an assessment of the risk and damage arising from the installation and use of such device has been submitted before the determination of the authorization; and
- (B) the address and if ascertainable, the owner, tenant and occupier of such property must be specified in the authorization; and
- (ii) in the case of Type 1 surveillance, the entry, by the use of reasonable force if necessary, onto the premises, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization provided that an assessment of the risk and damage arising from the entry has been submitted before the determination of the authorization;
- (b) where subsection (2)(b) is applicable –
- (i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization in or on the object, or an object of the class, specified in the prescribed authorization provided that if the surveillance device is to be installed or used in any private property –
- (A) an assessment of the risk and damage arising from the installation and use of such device has been submitted before the determination of the authorization; and
- (B) the address and if ascertainable, the owner, tenant and occupier of such property must be specified in the authorization; and
- (ii) in the case of Type 1 surveillance, the entry, by the use of reasonable force if necessary, onto any premises where the object, or an object of the class, is reasonably believed to be or likely to be, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization provided that an assessment of the risk and damage arising from the entry has been submitted before the determination of the authorization; and
- (c) where subsection (2)(c) is applicable –
- (i) the installation, use and maintenance of any of the surveillance devices authorized to be used under the prescribed authorization, in or on any

premises where the person specified in the prescribed authorization is reasonably believed to be or likely to be provided that if the surveillance device is to be installed or used in any private property –

- (A) an assessment of the risk and damage arising from the installation and use of such device has been submitted before the determination of the authorization; and
- (B) the address and if ascertainable, the owner, tenant and occupier of such property must be specified in the authorization ; and

- (ii) in the case of Type 1 surveillance, the entry, by the use of reasonable force if necessary, onto the premises, and onto any other premises adjoining or providing access to the premises, in order to carry out any conduct authorized or required to be carried out under the prescribed authorization provided that an assessment of the risk and damage arising from the entry has been submitted before the determination of the authorization.

(8) A prescribed authorization may contain terms that authorize the undertaking of the following conduct, that is necessary for and incidental to the carrying out of what is authorized or required to be carried out under the prescribed authorization –

- (a) the installation, use, maintenance and retrieval of any enhancement equipment for the devices;
- (b) the temporary removal of any conveyance or object from any premises for the installation, maintenance or retrieval of the devices or enhancement equipment and the return of the conveyance or object to the premises;
- (c) the breaking open of anything for the installation, maintenance or retrieval of the devices or enhancement equipment;
- (d) the connection of the devices or enhancement equipment to any source of electricity and the use of electricity from that source to operate the devices or enhancement equipment;
- (e) the connection of the devices or enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the devices or enhancement equipment; and
- (f) the provision of assistance for the execution of the prescribed authorization, provided that an assessment of the risk and damage arising from the above conduct has been submitted before the determination of the authorization.

30. What a prescribed authorization ~~further also~~ authorizes

A prescribed authorization ~~further also~~ authorizes the the retrieval of any of the devices authorized to be used under the prescribed authorization ~~undertaking of any conduct which it conduct, including the following conduct, that is necessary to undertake in order to~~ for and incidental to the carrying out of what is authorized

or required to be carried out under the prescribed authorization, and, without limiting the generality of the foregoing, such conduct includes –

- ~~(a) the retrieval of any of the devices authorized to be used under the prescribed authorization;~~
- ~~(b) the installation, use, maintenance and retrieval of any enhancement equipment for the devices;~~
- ~~(c) the temporary removal of any conveyance or object from any premises for the installation, maintenance or retrieval of the devices or enhancement equipment and the return of the conveyance or object to the premises;~~
- ~~(d) the breaking open of anything for the installation, maintenance or retrieval of the devices or enhancement equipment;~~
- ~~(e) the connection of the devices or enhancement equipment to any source of electricity and the use of electricity from that source to operate the devices or enhancement equipment;~~
- ~~(f) the connection of the devices or enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the devices or enhancement equipment; and~~
- ~~(g) the provision of assistance for the execution of the prescribed authorization.~~

30A. What a prescribed authorization may not authorize

(1) Notwithstanding anything in this Ordinance, unless exceptional circumstances exist –

- (a) no prescribed authorization may contain terms that authorize the interception of communications by reference to –
 - (i) in the case of a postal interception, an office or other relevant premises, or a residence, of a lawyer; or
 - (ii) in the case of a telecommunications interception, any telecommunications service used at an office or other relevant premises, or a residence, of a lawyer, or any telecommunications service known or reasonably expected to be known by the applicant to be ordinarily used by a lawyer for the purpose of providing legal advice to clients; and
- (b) no prescribed authorization may contain terms that authorize any covert surveillance to be carried out in respect of oral or written communications taking place at an office or other relevant premises, or a residence, of a lawyer.

(2) For the purposes of subsection (1), exceptional circumstances exist if the relevant authority is satisfied that there are reasonable grounds to believe –

- (a) that –
 - (i) the lawyer concerned;

- (ii) in the case of an office or other relevant premises of the lawyer, any other lawyer practising with him or any other person working in the office; or
- (iii) in the case of a residence of the lawyer, any other person residing in the residence, is a party to any activity which constitutes or would constitute a serious crime or a threat to public security; or
- (b) that any of the communications concerned is for the furtherance of a criminal purpose.
- (3) For the avoidance of doubt, a prescribed authorization does not authorize any device to be implanted in, or administered to, a person without the consent of the person **in writing**.
- (4) In this section –
 - “lawyer” (律師) means a barrister, solicitor or foreign lawyer as defined in section 2(1) of the Legal Practitioners Ordinance (Cap. 159) who practices as such, or any person holding an appointment under section 3(1) of the Legal Aid Ordinance (Cap. 91);
 - “other relevant premises” (其他有關處所), in relation to a lawyer, means any premises, other than an office of the lawyer, that are known or reasonably expected to be known by the applicant to be ordinarily used by the lawyer and by other lawyers for the purpose of providing legal advice to clients.

31. Prescribed authorization may be issued or renewed subject to conditions

(1) A prescribed authorization may be issued or renewed subject to any conditions specified in it that apply to the prescribed authorization itself or to any further authorization or requirement under it (whether granted or imposed under its terms or any provision of this Ordinance).

(2) *In the case of non-compliance with the specified conditions in subsection (1), the prescribed authorization shall cease to have effect from the time of non-compliance.*

Device retrieval warrants after prescribed authorizations having ceased to have effect

32. Application for device retrieval warrant

(1) Where a prescribed authorization has in any way ceased to have effect under this Ordinance, an officer of the department concerned may apply to a panel judge of the Court of First Instance for the issue of a device retrieval warrant authorizing the retrieval of any of the devices authorized to be used under the prescribed authorization if such devices –

- (a) have been installed in or on any premises or object, pursuant to the prescribed authorization; and
- (b) are still in or on such premises or object, or are in or on any other

premises or object.

(2) The application is –

(aa) to be made ex parte;

(a) to be made in writing; and

(b) to be supported by –

(i) a copy of the prescribed authorization; and

(ii) an affidavit of the applicant which is to comply with the requirements specified in Schedule 4.

33. Determination of application for device retrieval warrant

(1) Upon considering an application for the issue of a device retrieval warrant made under section 32, the ~~panel~~ judge of the Court of First Instance may, subject to subsection (2) –

(a) issue the device retrieval warrant sought under the application, with or without variations; or

(b) refuse to issue the device retrieval warrant.

(1A) When considering the application in subsection (1), the judge of the Court of the First Instance shall take into account the assessment of the risk and damage arising from the retrieval of such device to the premise or object.

(1B) If the judge of the Court of First Instance refuses to issue the device retrieval warrant in subsection (1)(b), he shall make an order directing the relevant head of the department to disable the function of the device.

(2) The ~~panel~~ judge of the Court of First Instance shall not issue the device retrieval warrant unless he is satisfied that section 32(1)(a) and (b) applies to the devices concerned.

(3) The ~~panel~~ judge of the Court of First Instance shall deliver his determination under subsection (1) by –

(a) in the case of subsection (1)(a), issuing the device retrieval warrant in writing with reason; or

(b) in the case of subsection (1)(b), giving the reason for the refusal in writing.

34. Duration of device retrieval warrant

A device retrieval warrant –

(a) takes effect at the time specified by the ~~panel~~ judge of the Court of First Instance when issuing the warrant, which in any case is not to be earlier than the time when it is issued; and

(b) ceases to have effect upon the expiration of the period specified by the ~~panel~~ judge of the Court of First Instance when issuing the warrant, which in any case is not to be longer than the period of 3 months beginning with the time when it takes effect.

35. What a device retrieval warrant may authorize under or by virtue of its terms, etc.

(1) A device retrieval warrant may authorize the retrieval of any devices specified in the warrant.

(2) A device retrieval warrant may contain terms that authorize the doing of anything reasonably necessary to conceal any conduct authorized to be carried out under the warrant, provided that an assessment of the risk and damage arising from the concealment has been submitted before the determination of the authorization and that the nature of concealment so authorized must be specified in the authorization.

(3) A device retrieval warrant may, if it is reasonably necessary for the execution of the warrant, contain terms that authorize the interference with any property (whether or not of any person who is the subject of the interception or covert surveillance concerned) provided that an assessment of the risk and damage arising from the interference with any property has been submitted before the determination of the authorization and that the nature of interference so authorized must be specified in the authorization.

36. What a device retrieval warrant ~~further also authorizes~~ may authorize or require under or by virtue of its terms, etc.

(1) A device retrieval warrant ~~further also authorizes~~ may contain terms that authorize the undertaking of ~~any conduct which it is necessary to undertake in order to carry out conduct, including the following conduct, that is necessary for and incidental to the carrying out of~~ what is authorized to be carried out under the warrant ~~and, without limiting the generality of the foregoing, such conduct includes –~~

- (a) the retrieval of any enhancement equipment for the devices authorized to be retrieved under the warrant;
- (b) the entry, by the use of reasonable force if necessary, onto any premises where the devices or enhancement equipment is reasonably believed to be or likely to be, and onto any other premises adjoining or providing access to the premises, in order to retrieve the devices or enhancement equipment;
- (c) the temporary removal of any conveyance or object from any premises for the retrieval of the devices or enhancement equipment and the return of the conveyance or object to the premises;
- (d) the breaking open of anything for the retrieval of the devices or enhancement equipment; and
- (e) the provision of assistance for the execution of the warrant,

provided that an assessment of the risk and damage arising from the above conduct has been submitted before the determination of the authorization.

(2) A device retrieval warrant which authorizes the retrieval of any tracking devices also authorizes the use of the tracking devices and any enhancement equipment for the tracking devices solely for the purposes of the location and retrieval

of the tracking devices or enhancement equipment.

37. Device retrieval warrant may be issued subject to conditions

(1) A device retrieval warrant may be issued subject to any conditions specified in it that apply to the warrant itself or to any further authorization under it (whether granted under its terms or any provision of this Ordinance).

(2) In the case of non-compliance with the specified conditions in subsection (1), the warrant shall cease to have effect from the time of non-compliance.

PART 4

THE COMMISSIONER

Division 1 – The Commissioner and his Functions

38. The Commissioner

(1) There is hereby established an office by the name of the Commissioner on Interception of Communications and Surveillance.

(2) The Chief Executive shall, on the recommendation of the Chief Justice, subject to the approval of the Legislative Council, appoint an eligible judge to be the Commissioner.

(3) The Commissioner shall be appointed for a period of 3 years, ~~and may from time to time be reappointed.~~

(4) The Commissioner shall be entitled to such remuneration and allowances as are determined by the Chief Executive.

(5) The Chief Executive may, on the recommendation of the Chief Justice, subject to the approval of the Legislative Council, revoke the appointment of the Commissioner for good cause.

(5A) A person previously appointed as the Commissioner may from time to time be further appointed as such in accordance with the provisions of this Ordinance that apply to the appointment of the Commissioner.

(6) In this section, “eligible judge” (合資格法官) means –

- (a) a Justice of Appeal of the Court of Appeal;
- (b) a judge of the Court of First Instance;
- (c) a former permanent judge of the Court of Final Appeal;
- (d) a former Justice of Appeal of the Court of Appeal; or
- (e) a former judge of the Court of First Instance.

39. Functions of Commissioner

The functions of the Commissioner are –

- (a) to oversee the overall implementation of this Ordinance (except the functioning of the Court of First Instance and the District Court relating to this Ordinance) and compliance by departments and their officers with the relevant requirements; and
- (b) without limiting the generality of paragraph (a), to –

- (i) conduct reviews under Division 2;
- (ii) carry out examinations under Division 3;
- (iia) investigate complaints made by any person in relation to any interception or surveillance carried out whether with or without authorization under Division 3A;
- (iib) give notifications to relevant persons under Division 3AB;
- (iii) submit reports to the Chief Executive and make recommendations to the Secretary for Security and heads of departments under Division 4;
- (iv) perform any further functions prescribed by regulation made under section 62 for the purposes of this subparagraph; and
- (v) perform such other functions as are imposed or conferred on him under this Ordinance or any other enactment.

Division 2 – Reviews by Commissioner

40. Reviews on compliance with relevant requirements

(1) The Commissioner shall conduct such reviews as he considers necessary on compliance by departments and their officers with the relevant requirements.

(1A) Without limiting the generality of subsection (1), the Commissioner shall conduct reviews on cases in respect of which a report has been submitted to him under section 23(3)(b), ~~26(3)(b)(ii)~~ or 52.

(2) Upon the conduct of any review under subsection (1) or (1A), the Commissioner shall record in writing –

- (a) details, as identified in the review, of any case of failure by any department or any of its officers to comply with any relevant requirement; and
- (b) any other finding he has made in the review.

41. Notifications to departments concerned, etc.

(1) The Commissioner shall notify the head of any department concerned of his findings in a review under section 40(2).

(2) On being notified of the findings of the Commissioner under subsection (1), the head of the department shall submit to the Commissioner a report with details of any measures taken by the department (including any disciplinary action taken in respect of any officer) to address any issues identified in the findings, as soon as reasonably practicable after the notification or, where the Commissioner has specified any period for submission of the report when giving the notification, within that period.

(3) Without prejudice to sections 47 and 48, the Commissioner may, whether before or after the head of the department has submitted a report to him under subsection (2), refer the findings and any other matters he thinks fit to the Chief Executive ~~or the Secretary for Justice or both~~ or any panel judge of the Court of

First Instance or any or all of them.

Division 3 – Examinations by Commissioner

42. Application for examination

(1) A person may apply to the Commissioner for an examination under this Division, if he ~~believes~~ suspects –

- (a) that any communication transmitted to or by him has been intercepted by a department; ~~or~~
- (b) that he is the subject of any covert surveillance that has been carried out by a department; or
- (c) that he has sustained any damage arising from any interception or covert surveillance that has been carried out by a department.

(2) The application is to be made in writing.

43. Examination by Commissioner

(1) Where the Commissioner in the course of performing any of his functions under this Ordinance considers or suspects that there is any case in which any interception or covert surveillance has been carried out in contravention of this Ordinance, or receives an application under section ~~s~~ 42(1)(a) and (b), he shall, subject to section 44, carry out an examination to determine –

- (a) whether or not the interception or covert surveillance alleged has taken place; and
- (b) if so, whether or not ~~a prescribed authorization should have been, but has not been, issued or renewed under this Ordinance in relation to the interception or covert surveillance alleged.~~ the interception or covert surveillance alleged has been carried out without the authority of a prescribed authorization issued or renewed under this Ordinance.

(1A) Where the Commissioner in the course of performing any of his functions under this Ordinance considers or suspects that there is any case in which any interception or covert surveillance has been carried out in contravention of this Ordinance, or receives an application under section 42(1)(c), he shall, subject to section 44, carry out an examination to determine –

- (a) whether or not the interception or covert surveillance alleged has taken place; and
- (b) if so, whether or not the applicant has sustained damages arising from any interception or covert surveillance carried out by a department.

(2) In the case of subsection (1), if, ~~if,~~ on an examination, the Commissioner determines that the interception or covert surveillance alleged has been carried out without the authority of a prescribed authorization issued or renewed under this Ordinance, he shall give notice to the applicant –

- (a) stating that –
 - (i) he has found the case in the applicant's favour and indicating whether the case is one of interception or covert surveillance;
 - (ii) the broad nature of the interception or covert surveillance;
 - (iii) the time when the interception or covert surveillance commences and the time when the interception or covert surveillance ends; and
 - (iv) the duration of the interception or covert surveillance; and
- (b) inviting the applicant to confirm whether the applicant wishes to seek an order for the payment of compensation under the application, and if so, to make written submissions to him for that purpose. a prescribed authorization should have been, but has not been, issued or renewed under this Ordinance in relation to the interception or covert surveillance alleged, he –
- (a) ~~shall give notice to the applicant stating that he has found the case in the applicant's favour; and~~
- (b) ~~may, if he thinks fit, make an order for the payment of compensation by the Government to the applicant.~~

(2A) In the case of subsection (1A), if, on an examination, the Commissioner determines that the interception or covert surveillance alleged has been carried out and that the applicant has sustained damages arising from the alleged interception or covert surveillance, he shall give notice to the applicant –

- (a) stating that he has found the case in the applicant's favour; and
- (b) inviting the applicant to confirm whether the applicant wishes to seek an order for the payment of compensation under the application, and if so, to make written submissions to him for that purpose.

(2BA) Upon receiving confirmation from the applicant that an order for the payment of compensation is sought, the Commissioner, upon taking into account any written submissions made to him for that purpose, may make any order for the payment of compensation by the Government to the applicant.

(2CB) The compensation ordered to be paid under subsection (2BA) may include compensation for injury of feelings.

(3) If, on an examination, the Commissioner makes a determination other than that referred to in subsections (2) or (2A), he shall give notice to the applicant stating that he has not found the case in the applicant's favour.

~~(4) The compensation ordered to be paid under subsection (2)(b) may include compensation for injury to feelings.~~

(5) Notwithstanding subsections (2), (2A), (2B) and (3), the Commissioner shall not give any notice or make any order under those subsections for so long as he considers that the giving of the notice or the making of the order (as the case may be) would be prejudicial to the prevention or detection of crime or the protection of public

security.

(6) The Commissioner shall not make a determination referred to in subsections (2) or (2A) in respect of an interception if the interception is within the description of section 4(2)(b) or (c).

44. Grounds for not carrying out examination, etc.

(1) Where, before or in the course of an examination, the Commissioner considers –

- (a) that the application for the examination is received by the Commissioner more than ~~1 year~~ 5 years after the day on which the interception or covert surveillance is alleged to have taken place or, where the interception or covert surveillance is alleged to have taken place on more than 1 day, the last occasion on which it is alleged to have taken place, and that it is not unfair for him not to carry out the examination;
- (b) that the application is made anonymously;
- (c) that the applicant cannot, after the use of reasonable efforts, be identified or traced; or
- (d) that, having regard to all the circumstances of the case, the application is frivolous or vexatious or is not made in good faith, the Commissioner may refuse to carry out the examination or, where the examination has been commenced, to proceed with the carrying out of the examination (including the making of any determination further to the examination).

~~(2) Where, before or in the course of an examination, the Commissioner is satisfied that any relevant criminal proceedings are pending or are likely to be instituted, the Commissioner shall not carry out the examination or, where the examination has been commenced, proceed with the carrying out of the examination (including the making of any determination further to the examination) –~~

- ~~(a) in the case of any pending criminal proceedings, until they have been finally determined or finally disposed of; or~~
- ~~(b) in the case of any criminal proceedings which are likely to be instituted, until they have been finally determined or finally disposed of or, if applicable, until they are no longer likely to be instituted.~~

~~(3) For the purposes of subsection (2), criminal proceedings are, in relation to an examination, regarded as relevant if, but only if, the interception or covert surveillance alleged in the application for the examination is or may be relevant to the determination of any question concerning any evidence which has been or may be adduced in those proceedings.~~

45. Further provisions relating to examinations

(1) For the purposes of an examination, ~~the Commissioner shall –~~

- ~~(a) except as otherwise provided in this Ordinance, in determining whether any interception or covert surveillance has been carried out without the authority of a prescribed authorization issued or renewed under this~~

~~Ordinance, the Commissioner shall apply the principles applicable by a court on an application for judicial review; and~~
 (b) and subject to section 51(1), the Commissioner shall carry out the examination on the basis of written submissions made to him.

(2) Without prejudice to section 51(3), for the purposes of an examination, the applicant is not entitled to have access to any information, document or other matter compiled by, or made available to, the Commissioner in connection with the examination.

(3) Without prejudice to section 43(5), in giving notice to an applicant or making any order under section 43(2)(~~a~~), (2A), (2B) or (3), the Commissioner shall not –

- (a) give reasons for his determination;
- (b) give details of any interception or covert surveillance concerned further to those mentioned in sections 43(2)(a) or (2A)(a); and or
- (c) in the case of section 43(3), indicate whether or not the interception or covert surveillance alleged has taken place,

if the giving of the information under subsections (a), (b) and (c) would be prejudicial to the prevention or detection of crime or the protection of public security.

46. Notifications to departments concerned, etc.

(1) Where, on an examination, the Commissioner makes a determination ~~under~~ referred to in sections 43(2) or 43(2A), he shall notify the head of the department concerned of the determination, including any order or findings he has made in the examination.

(2) On being ~~notified of the determination given the notification~~ under subsection (1), the head of the department shall submit to the Commissioner a report with details of any measures taken by the department (including any disciplinary action taken in respect of any officer) to address any issues arising from the determination, as soon as reasonably practicable after the notification or, where the Commissioner has specified any period for submission of the report when giving the notification, within that period.

(3) Without prejudice to sections 47 and 48, the Commissioner may, whether before or after the head of the department has submitted a report to him under subsection (2), refer the determination and any other matters he thinks fit to the Chief Executive or, the Secretary for Justice or both any panel judge of the Court of First Instance or any or all of them.

Division 3A – Powers of Commissioner

46A. Powers of Commissioner

The Commissioner shall have a general power –

(a) to investigate any complaint of alleged cases of interception or covert

- surveillance;.
- (b) to require any department to investigate any person within that department, if he has reasonable grounds to believe that the person –
- (i) has provided false and misleading information in obtaining an authorization;or
 - (ii) has contravened provisions of this Ordinance,
- and to require a report from such department on the outcome of any investigation and any disciplinary action taken;
- (c) to investigate any complaint by any person alleged to have been aggrieved or adversely affected by –
- (i) the execution of any prescribed authorization;
 - (ii) any interception of covert surveillance without the authority of a prescribed authorization or in excess of any prescribed authorization;and
- (d) to conduct any investigation (including criminal, administrative and disciplinary) as he considers necessary into the conduct of any, person, apart from a judge of the Court of First Instance or a judge of the District Court, and refer any matter to the Director of Public Prosecutions upon conclusion of such investigation .

Division 3A~~B~~ – Notifications by Commissioner

46A~~B~~. Notifications to relevant persons

(1) If, in the course of performing any of his functions under this Ordinance, the Commissioner considers that there is any case in which any interception or covert surveillance –

- has been carried out by a department without the authority of a prescribed authorization issued or renewed under this Ordinance;
 - (c) has been carried out by a department mistakenly or wrongfully;or
 - (d) has been carried out by a department in contravention of this Ordinance , subject to subsection (6), the Commissioner shall give notice to the relevant person –
- (a) stating that –
 - (i) there has been such a case and indicating whether the case is one of interception or covert surveillance;
 - (ii) the broad nature of the interception or covert surveillance;
 - (iii) the time when the interception or covert surveillance commences and the time when the interception or covert surveillance ends; and
 - (iv) the duration of the interception or covert surveillance; and
 - (b) informing the relevant person of his right to apply to the Commissioner for an examination in respect of the interception or covert surveillance.

(2) Where the relevant person makes an application for an examination in respect of the interception or covert surveillance within 6 months after receipt of the notice or within such further period as the Commissioner may allow, the Commissioner shall, notwithstanding anything in section 44(1)(a) but subject to the other provisions of section 44, make a determination referred to in sections 43(2) or 43(2A), and the provisions of this Ordinance are to apply accordingly.

(3) Notwithstanding subsection (1), the Commissioner shall not give any notice under that subsection for so long as he considers that the giving of the notice would be prejudicial to the prevention or detection of crime or the protection of public security.

(4) Without prejudice to subsection (3), in giving notice to a relevant person under subsection (1), the Commissioner shall not –

(a) give reasons for his findings; or

(b) give details of any interception or covert surveillance concerned further to those mentioned in subsection (1)(a).

(5) For the purposes of this section, in considering whether any interception or covert surveillance has been carried out without the authority of a prescribed authorization issued or renewed under this Ordinance, the Commissioner shall apply the principles applicable by a court on an application for judicial review.

(6) This section does not require the Commissioner to give any notice to a relevant person if –

(a) the relevant person cannot, after the use of reasonable efforts, be identified or traced;

(b) the Commissioner considers that the intrusiveness of the interception or covert surveillance concerned on the relevant person is negligible; or

(c) in the case of interception, it is within the description of section 4(2)(b) or (c).

(7) In this section, “relevant person” (有關人士) means any person who is the subject of the interception or covert surveillance concerned.

Division 4 – Reports and Recommendations by Commissioner

47. Annual reports to Chief Executive by Commissioner

(1) The Commissioner shall, for each report period, submit a report to the Chief Executive.

(2) A report for a report period is to set out, separately in relation to interception and covert surveillance –

(a) a list showing –

(i) the respective numbers of judge’s authorizations, executive authorizations and emergency authorizations issued under this Ordinance during the report period, and the average duration of the respective prescribed authorizations;

(ii) the respective numbers of judge’s authorizations and executive authorizations renewed under this Ordinance

- during the report period, and the average duration of the respective renewals;
- (iii) the respective numbers of judge's authorizations, executive authorizations and emergency authorizations issued as a result of an oral application under this Ordinance during the report period, and the average duration of the respective prescribed authorizations;
 - (iv) the respective numbers of judge's authorizations and executive authorizations renewed as a result of an oral application under this Ordinance during the report period, and the average duration of the respective renewals;
 - (v) the respective numbers of judge's authorizations and executive authorizations that have been renewed under this Ordinance during the report period further to 5 or more previous renewals;
 - (vi) the respective numbers of applications for the issue of judge's authorizations, executive authorizations and emergency authorizations made under this Ordinance that have been refused during the report period;
 - (vii) the respective numbers of applications for the renewal of judge's authorizations and executive authorizations made under this Ordinance that have been refused during the report period;
 - (viii) the respective numbers of oral applications for the issue of judge's authorizations, executive authorizations and emergency authorizations made under this Ordinance that have been refused during the report period; and
 - (ix) the respective numbers of oral applications for the renewal of judge's authorizations and executive authorizations made under this Ordinance that have been refused during the report period;
 - (x) the respective number of issued or renewed authorization for the purpose of preventing and detecting of serious crimes, and issued or renewed authorization for the purpose of protecting public security during the report period;.
 - (xi) the total number of telephone lines intercepted during the report period;
 - (xii) the total number of facsimile lines intercepted during the report period;
 - (xiii) total number of email accounts intercepted during the report period;
 - (xiv) the total number of Internet Protocol (IP) addresses

under surveillance during the report period;
(xv) the total number of persons who have been the subjects
of surveillance during the report period;
(xvi) the total number of premises under surveillance during
the report period.

~~(a) a list showing—~~

- ~~(i) the number of prescribed authorizations issued under this Ordinance during the report period, and the average duration of the prescribed authorizations;~~
- ~~(ii) the number of prescribed authorizations renewed under this Ordinance during the report period, and the average duration of the renewals;~~
- ~~(iii) the number of applications for the issue of prescribed authorizations made under this Ordinance that have been refused during the report period; and~~
- ~~(iv) the number of applications for the renewal of prescribed authorizations made under this Ordinance that have been refused during the report period;~~

—

(b) a list showing –

- (i) the major categories of offences for the investigation of which prescribed authorizations have been issued or renewed under this Ordinance during the report period; ~~and~~
(ia) the major categories of threats to public security of which prescribed authorizations have been issued or renewed under this Ordinance during the report period; and
- (ii) the number of persons arrested during the report period as a result of or further to any interception or covert surveillance carried out pursuant to a prescribed authorization;

(c) a list showing –

- (i) the number of device retrieval warrants issued under this Ordinance during the report period, and the average duration of the warrants; and
- (ii) the number of applications for the issue of device retrieval warrants made under this Ordinance that have been refused during the report period;

(d) a list showing –

- (i) a summary of reviews conducted by the Commissioner under section 40 during the report period;
- (ii) the number and broad nature of any cases of irregularities or errors identified in the reviews during the report period;

- (iii) the number of applications for examination that have been received by the Commissioner during the report period;
- (iv) ~~the respective numbers of notices given by the Commissioner under section 43(2) and section 43(3) during the report period further to examinations; a summary of the determinations of the Commissioner on examinations carried out during the report period; and~~
- (iva) the number of cases in which a notice has been given by the Commissioner under section 46A during the report period;
- (v) the broad nature of recommendations made by the Commissioner under sections 48, 49 and 50 during the report period; and
- (vi) the *respective* number of cases in which information subject to legal professional privilege *and in which content of journalistic material have* has been obtained in consequence of any interception or covert surveillance carried out pursuant to a prescribed authorization during the report period; and
- (vii) the *respective* number of cases of different departments in which disciplinary action has been taken in respect of any officer of a department according to any report submitted to the Commissioner under section 41, 46 or 50 during the report period, and the broad nature of such action; and
- (e) an assessment on the overall *implementation of this Ordinance and the overall* compliance with the relevant requirements during the report period.

(3) The report is to be submitted within 6 months after the expiry of the report period.

(4) ~~Subject to subsection (5), the Chief Executive shall cause a copy of the report to be laid on the table of the Legislative Council.~~ The Chief Executive shall cause to be laid on the table of the Legislative Council a copy of the report, together with a statement as to whether any matter has been excluded from that copy under subsection (5) without the agreement of the Commissioner.

(5) If the Chief Executive considers that the publication of any matter in the report referred to in subsection (4) would be prejudicial to the prevention or detection of crime or the protection of public security, he may, after consultation with the Commissioner, exclude such matter from the copy of the report to be laid on the table of the Legislative Council under that subsection.

(5A) The matter excluded in subsection (5) shall be reported to the Legislative Council under confidential cover.

(6) In this section, “report period” (報告期間), in relation to a report required to be submitted under subsection (1), means –

- (a) the period beginning on the commencement of this Ordinance and ending on 31 December in the same year; or
- (b) any of the succeeding periods of 12 months ending on 31 December.

48. Other reports to Chief Executive by Commissioner

(1) In addition to any report required to be submitted to the Chief Executive under section 47, the Commissioner may from time to time submit any further report to the Chief Executive on any matter relating to the performance of his functions under this Ordinance as he thinks fit.

(2) The Chief Executive shall cause to be laid on the table of the Legislative Council a copy of the report, together with a statement as to whether any matter has been excluded from that copy under subsection (3) without the agreement of the Commissioner.

(3) If the Chief Executive considers that the publication of any matter in the report referred to in subsection (2) would be prejudicial to the prevention or detection of crime or the protection of public security, he may, after consultation with the Commissioner, exclude such matter from the copy of the report to be laid on the table of the Legislative Council under that subsection.

(4) The matter excluded in subsection (3) shall be reported to the Legislative Council under confidential cover.

49. Recommendations to Secretary for Security on code of practice

(1) If, in the course of performing any of his functions under this Ordinance, the Commissioner considers that any provision of the code of practice should be revised to better carry out the objects of this Ordinance, he may make such recommendations to the Secretary for Security as he thinks fit.

(2) Where the Commissioner makes any recommendations to the Secretary for Security under subsection (1), the Secretary shall notify the Commissioner and the Legislative Council of any exercise of power by him under section 59(3) to implement the recommendations, as soon as reasonably practicable after the recommendations have been made or, where the Commissioner has specified any period for the issue of the notification when making the recommendations, within that period.

50. Recommendations to departments

(1) If, in the course of performing any of his functions under this Ordinance, the Commissioner considers that any arrangements made by any department should be changed to better carry out the objects of this Ordinance or the provisions of the code of practice, he may make such recommendations to the head of the department as he thinks fit.

(2) Where the Commissioner makes any recommendations to the head of the

department under subsection (1), the head of the department shall submit to the Commissioner a report with details of any measures taken by the department (including any disciplinary action taken in respect of any officer) to implement the recommendations, as soon as reasonably practicable after the recommendations have been made or, where the Commissioner has specified any period for submission of the report when making the recommendations, within that period.

(2A) The Commissioner shall cause to be laid on the table of the Legislative Council a copy of the report, together with a statement as to whether any matter has been excluded from that copy under subsection (2B).

(2B) If the Commissioner considers that the publication of any matter in the report referred to in subsection (2A) would be prejudicial to the prevention or detection of crime or the protection of public security, he may exclude such matter from the copy of the report to be laid on the table of the Legislative Council under that subsection.

(2C) The matter excluded in subsection (2B) shall be reported to the Legislative Council under confidential cover.

(3) Without prejudice to sections 47 and 48, the Commissioner may, whether before or after the head of the department has submitted a report to him under subsection (2), refer the recommendations and any other matters he thinks fit to the Chief Executive ~~or~~, the Secretary for Justice ~~or both or any panel judge~~ of the Court of First Instance or any or all of them.

Division 5 – Further Provisions Relating to Performance of Functions by Commissioner

51. Further powers of Commissioner

(1) For the purpose of performing any of his functions under this Ordinance, the Commissioner may –

(a) require any public officer or any other person, apart from any judge to answer any question, and to provide any information, document or other matter in his possession or control to the Commissioner, within the time and in the manner specified by the Commissioner when making the requirement; ~~and~~

(b) require any officer of a department to prepare any report on any case of interception or covert surveillance handled by the department, or on any class of such cases, within the time and in the manner specified by the Commissioner when making the requirement; and

(c) .require any head of department to take such remedial action and make compensation as he considers reasonable and necessary.

(1A) Non compliance with subsection (1A) shall be an offence with maximum penalty of 2 years imprisonment.

(1AB) For the purpose of performing any of his functions under this Ordinance, the Commissioner may request a panel judge to provide him with access to any of the

documents or records kept under section 3 of Schedule 2.

(2) Notwithstanding any other provision of this Ordinance or any other law, any person on whom a requirement is imposed by the Commissioner under subsection (1) shall comply with the requirement.

(3) Except as otherwise provided in this Ordinance, the Commissioner shall not be required to produce in any court or to divulge or communicate to any court, or to provide or disclose to any person, any information, document or other matter compiled by, or made available to, him in the course of performing any of his functions under this Ordinance.

(4) Except as otherwise provided in this Ordinance, the Commissioner may determine the procedure to be adopted in performing any of his functions under this Ordinance.

52. General obligations of departments to report on non-compliance

Without prejudice to other provisions of this Part, where the head of any department considers that there may have been any case of —

(a) failure by the department or any of its officers to comply with any relevant requirement;

(b) contravention against this Ordinance; or

(c) submission of misleading and false information for the purpose of obtaining a prescribed authorization or for the purpose of implementing any provision of this Ordinance,

he shall submit to the Commissioner a report with details of the case.

53. Commissioner not regarded as court

In performing any of his functions under this Ordinance, the Commissioner is for all purposes not regarded as a court or a member of a court.

PART 5 FURTHER SAFEGUARDS

54. Regular reviews

(1) The head of each department shall make arrangements to keep under regular review the compliance by officers of the department with the relevant requirements.

(2) Without prejudice to subsection (1), where the head of any department has made any designation under section 7, he shall make arrangements for officers of a rank higher than those held by the authorizing officers of the department to keep under regular review the performance by the authorizing officers of any function under this Ordinance.

55. Discontinuance of interception or covert surveillance

(1) If, ~~in the course of or further to any regular review conducted under section~~

~~54(1) or (2)~~, the officer by whom ~~the~~ any regular review is or has been conducted under section 54(1) or (2) is of the opinion that ~~any-the~~ ground for discontinuance of a prescribed authorization exists, he shall, as soon as reasonably practicable after forming the opinion, cause the interception or covert surveillance concerned to be discontinued.

(2) Without prejudice to subsection (1), where a prescribed authorization has been issued or renewed under this Ordinance, the officer of the department concerned who is for the time being in charge of the interception or covert surveillance concerned –

- (a) shall, as soon as reasonably practicable after he becomes aware that ~~any-~~ the ground for discontinuance of the prescribed authorization exists, cause the interception or covert surveillance to be discontinued; and
- (b) may at any time cause the interception or covert surveillance to be discontinued.

(3) Where any officer has caused any interception or covert surveillance to be discontinued, whether under subsection (1) or (2), he shall, as soon as reasonably practicable after the discontinuance, cause a report on the discontinuance and the ground for the discontinuance to be provided to the relevant authority to whom an application under this Ordinance for the issue or renewal of the prescribed authorization concerned has last been made.

(4) Where the relevant authority receives a report under subsection (3), he shall, as soon as reasonably practicable after receiving the report, revoke the prescribed authorization concerned.

(5) Where any prescribed authorization is revoked under subsection (4), the prescribed authorization is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.

(5A) If, at the time of the provision of a report to the relevant authority under subsection (3), the relevant authority is no longer holding his office or performing the relevant functions of his office –

- (a) without prejudice to section 54 of the Interpretation and General Clauses Ordinance (Cap. 1), the reference to relevant authority in that subsection includes the person for the time being appointed as a panel judge or authorizing officer (as the case may be) and lawfully performing the relevant functions of the office of that relevant authority; and
- (b) the provisions of this section are to apply accordingly.

(6) For the purposes of this section, ~~a-the~~ ground for discontinuance of a prescribed authorization exists if –

- ~~(a)~~ (a) the conditions for the continuance of the prescribed authorization under section 3 are not met;
- (b) the specified conditions in section 31 are not met;
- (c) the application for, issuance or renewal of any prescribed authorization was in contravention of this Ordinance;
- (d) the interception or acts of covert surveillance carried out was in

excess of the prescribed authorization. ~~or~~

~~(b) the relevant purpose of the prescribed authorization has been achieved.~~

(7) In this section, “relevant duration provision” (有關時限條文) means section 10(b), 13(b), 16(b), 19(b) or 22(1)(b) (as may be applicable).

55A. Reports to relevant authorities following arrests

(1) Where, further to the issue or renewal of a prescribed authorization under this Ordinance, the officer of the department concerned who is for the time being in charge of the interception or covert surveillance concerned becomes aware that the subject of the interception or covert surveillance has been arrested, the officer shall, as soon as reasonably practicable after he becomes aware of the matter, cause to be provided to the relevant authority by whom the prescribed authorization has been issued or renewed a report assessing the effect of the arrest on the likelihood that any information which may be subject to legal professional privilege will be obtained by continuing the interception or covert surveillance.

(2) Where the relevant authority receives a report under subsection (1), he shall revoke the prescribed authorization if he considers that the conditions for the continuance of the prescribed authorization under section 3 or that the specified conditions under section 31 are not met.

(3) Where the prescribed authorization is revoked under subsection (2), the prescribed authorization is, notwithstanding the relevant duration provision, to cease to have effect from the time of the revocation.

(4) If, at the time of the provision of a report to the relevant authority under subsection (1), the relevant authority is no longer holding his office or performing the relevant functions of his office –

(a) without prejudice to section 54 of the Interpretation and General Clauses Ordinance (Cap. 1), the reference to relevant authority in that subsection includes the person for the time being appointed as a panel judge or authorizing officer (as the case may be) and lawfully performing the relevant functions of the office of that relevant authority; and

(b) the provisions of this section are to apply accordingly.

(5) In this section, “relevant duration provision” (有關時限條文) means section 10(b), 13(b), 16(b), 19(b) or 22(1)(b) (as may be applicable).

56. Safeguards for protected products

(1) Where any protected product has been obtained pursuant to any prescribed authorization issued or renewed under this Ordinance on an application by any officer of a department, the head of the department shall make arrangements to ensure –

(a) that the following are limited to the minimum that is necessary for the relevant purpose of the prescribed authorization –

(i) the extent to which the protected product is disclosed;

- (ii) the number of persons to whom any of the protected product is disclosed;
- (iii) the extent to which the protected product is copied; and
- (iv) the number of copies made of any of the protected product;
- (b) that all practicable steps are taken to ensure that the protected product is protected against unauthorized or accidental access, processing, erasure or other use; and
- (c) that the protected product is destroyed as soon as its retention is not necessary for the relevant purpose of the prescribed authorization.

(1A) Where any protected product described in subsection (1) contains any information that is subject to legal professional privilege, subsection (1)(c) is to be construed as also requiring the head of the department concerned to make arrangements to ensure that any part of the protected product that contains the information –

(a) in the case of a prescribed authorization for a postal interception or covert surveillance, is destroyed not later than 1 year after its retention ceases to be necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted; or

(b) in the case of a prescribed authorization for a telecommunications interception, is as soon as reasonably practicable destroyed.

(2) For the purposes of this section, something is necessary for the relevant purpose of a prescribed authorization –

(a) in the case of subsection (1)(a), if –

(i) it continues to be, or is likely to become, necessary for the relevant purpose; or

~~(b)~~(ii) except in the case of a prescribed authorization for a telecommunications interception, it is necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted; or.

(b) in the case of subsection (1)(c) –

(i) when it continues to be, or is likely to become, necessary for the relevant purpose; or

(ii) except in the case of a prescribed authorization for a telecommunications interception, at any time before the expiration of 1 year after it ceases to be necessary for the purposes of any civil or criminal proceedings before any court that are pending or are likely to be instituted.

57. Record keeping

(1) Without prejudice to section 56, each department shall keep a record which is to contain –

(a) in respect of each application for the issue or renewal of a prescribed

authorization under this Ordinance by any officer of the department, a record of –

- (i) the application (including a copy of any affidavit ~~or statement~~ provided under Part 3 for the purposes of the application); and
 - (ii) the determination in respect of the application by the relevant authority (including a copy of any prescribed authorization issued or renewed under Part 3 as a result of the application);
- (b) in respect of each application for confirmation of an emergency authorization by any officer of the department as provided for in section 23(1), a record of –
- (i) the application (including a copy of any affidavit provided under section 23(2)(b) ~~or, where section 28 applies, a copy of any record, affidavit or other document provided as described in section 28(1)(b),~~ for the purposes of the application); and
 - (ii) the determination in respect of the application by a ~~panel~~ judge of the Court of First Instance (including a copy of any endorsement made ~~or, where section 28 applies, a copy of any emergency authorization issued,~~ under section 24(5) as a result of the application);
- ~~(c) in respect of each application for confirmation of a prescribed authorization or renewal by any officer of the department as provided for in section 26(1), a record of –~~
- ~~(i) the application (including a copy of any record, affidavit or statement provided under section 26(2)(b) for the purposes of the application); and~~
 - ~~(ii) the determination in respect of the application by the relevant authority (including a copy of any prescribed authorization issued or renewed under section 27(5) as a result of the application);~~
- (d) a record of –
- (i) any case in which any interception or covert surveillance has been discontinued by any officer of the department under section 55; and (ii) any case in which any prescribed authorization has been revoked under section 55 further to the discontinuance;
- (e) in respect of each application for the issue of a device retrieval warrant under section 32 by any officer of the department, a record of –
- (i) the application (including a copy of any affidavit provided under section 32(2)(b) for the purposes of the application); and
 - (ii) the determination in respect of the application by a ~~panel~~ judge of the Court of First Instance (including a copy of any device retrieval warrant issued under section 33(3) as a result of the application);
- (f) a record of –

- (i) any case to which section 23(3) applies by reason that no application for confirmation of an emergency authorization is made within the period of 48 hours by any officer of the department;
 - ~~(ii) any case to which section 26(3) applies by reason that no application for confirmation of a prescribed authorization or renewal is made within the period of 48 hours by any officer of the department; and~~
 - (iii) any findings in respect of any other irregularities and errors identified or detected by any officer of the department, whether in any regular review conducted under section 54(1) and (2) or otherwise; and
 - (g) any record reasonably required to be kept by the department to enable the Commissioner to prepare reports for submission to the Chief Executive under section 47, or otherwise to perform any of his functions under this Ordinance.
- (2) The record kept under subsection (1) –
- (a) to the extent that it relates to any prescribed authorization or device retrieval warrant –
 - (i) is to be retained for a period of at least ~~2~~ 10 years after the day on which the prescribed authorization or device retrieval warrant (as the case may be) has ceased to have effect; and
 - (ii) without prejudice to subparagraph (i), where it has come to the notice of the department concerned that any relevant civil or criminal proceedings before any court are pending or are likely to be instituted, or any relevant review is being conducted under section 40, or, in the case of a prescribed authorization, any relevant application for an examination has been made under section 42, is to be retained –
 - (A) in the case of any pending proceedings, review or application, for a period of at least until 1 year after the pending proceedings, review or application has been finally determined or finally disposed of ~~or until the review has been completed or finally disposed of (as the case may be)~~; or
 - (B) in the case of any proceedings which are likely to be instituted, for a period of at least until 1 year after they have been finally determined or finally disposed of or, if applicable, for a period of until at least 1 year after they are no longer likely to be instituted; or
 - (b) to the extent that it does not relate to any prescribed authorization or device retrieval warrant, is to be retained for a period of at least ~~2~~ 10 years.

(3) For the purposes of subsection (2), any proceedings, review or application is, in relation to any part of a record that relates to any prescribed authorization or device retrieval warrant, regarded as relevant if, but only if –

- (a) the prescribed authorization or device retrieval warrant (as the case may be) is or may be relevant to the determination of any question for the purposes of the proceedings, review or application (as the case may be); or
- (b) in the case of a prescribed authorization, any protected product obtained pursuant to the prescribed authorization is or may be relevant to the determination of any question for the purposes of the proceedings, review or application (as the case may be).

~~58. Non-admissibility of telecommunications interception product~~

~~(1) Any telecommunications interception product shall not be admissible in evidence in any proceedings before any court other than to prove that a relevant offence has been committed.~~

~~(2) Any telecommunications interception product, and any particulars as to a telecommunications interception carried out pursuant to a relevant prescribed authorization, shall not be made available to any party to any proceedings before any court (other than any such proceedings instituted for a relevant offence).~~

~~(3) In any proceedings before any court (other than any such proceedings instituted for a relevant offence), any evidence or question which tends to suggest any of the following matters shall not be adduced or asked –~~

- ~~(a) that an application has been made for the issue or renewal of a relevant prescribed authorization, or the issue of a relevant device retrieval warrant, under this Ordinance;~~
- ~~(b) that a relevant prescribed authorization has been issued or renewed, or a relevant device retrieval warrant has been issued, under this Ordinance;~~
- ~~(c) that any requirement has been imposed on any person to provide assistance for the execution of a relevant prescribed authorization or a relevant device retrieval warrant;~~
- ~~(d) that any information has been obtained pursuant to a relevant prescribed authorization.~~

~~(4) Notwithstanding subsection (2), where, for the purposes of any criminal proceedings (whether being criminal proceedings instituted for an offence or any related proceedings), any information obtained pursuant to a relevant prescribed authorization and continuing to be available to the department concerned might reasonably be considered capable of undermining the case for the prosecution against the defence or of assisting the case for the defence –~~

- ~~(a) the department shall disclose the information to the prosecution; and~~
- ~~(b) the prosecution shall then disclose the information to the judge in an ex parte hearing that is held in private.~~

~~(4) This section is not to be construed as prohibiting the disclosure of any information that continues to be available for disclosure, to the extent that—~~
~~(a) the disclosure is made to ensure that a person conducting the prosecution of any offence has the information he needs to determine what is required of him by his duty to secure the fairness of the trial of that offence; or~~
~~(b) the disclosure is made to a judge alone in a case in which the judge has ordered the disclosure to be so made to him;~~
~~(5) A judge may only order a disclosure under subsection (4)(b) if he is satisfied that the disclosure is essential in the interests of justice.~~
~~(6) Where a judge orders a disclosure under subsection (4)(b), and in consequence of that disclosure he considers that it is essential in the interests of justice, he may—~~
~~The judge may, further to the disclosure to him of the information under subsection (4)(b), make such orders as he thinks fit for the purpose of securing the fairness of the proceedings.~~
~~direct the person conducting the prosecution of any offence to make for the purposes of the proceedings concerned any such admission of fact as the judge considers essential to secure the fairness of the trial of that offence.~~
~~(6A) Where any order is made under subsection (6) in any criminal proceedings, the prosecution shall disclose to the judge for any related proceedings the terms of the order and the information concerned in an ex parte hearing that is held in private.~~
~~(7) Notwithstanding subsection (6), no direction order made under that subsection authorizes or requires anything to be done in contravention of subsections (1), (2) and (3).~~
~~(8) In this section—~~
~~“judge” (法官), in relation to any proceedings, means the judge or magistrate before whom those proceedings are or are to be heard, or any other judge or magistrate having jurisdiction to deal with the matter concerned;~~
~~“party” (一方), in relation to any criminal proceedings, includes the prosecution;~~
~~“related proceedings” (—), in relation to any criminal proceedings, means any further proceedings (including appeal proceedings) arising from, or any proceedings preliminary or incidental to, those proceedings;~~
~~“relevant device retrieval warrant” (—有關器材取出手令) means a device retrieval warrant for the retrieval of any of the devices authorized to be used under a relevant prescribed authorization;~~
~~“relevant offence” (有關罪行) means any offence constituted by the disclosure of any telecommunications interception product or of any information relating to the obtaining of any telecommunications interception product (whether or not there are other constituent elements of the offence);~~
~~“relevant prescribed authorization” (—有關訂明授權) means a prescribed authorization for a telecommunications interception;~~
~~“telecommunications interception product” (—電訊截取成果) means any~~

~~interception product to the extent that it is~~

~~74~~

~~(a) any contents of a communication that have been obtained pursuant to a relevant prescribed authorization; or~~

~~(b) a copy of such contents.~~

58A. Information subject to legal professional privilege to remain privileged

Any information that is subject to legal professional privilege is to remain privileged notwithstanding that it has been obtained pursuant to a prescribed authorization.

59. Code of practice

(1) The Secretary for Security shall issue a code of practice for the purpose of providing practical guidance to officers of the departments in respect of matters provided for in this Ordinance.

(2) Without limiting the generality of subsection (1), the Secretary for Security may in the code of practice specify the form of any application to be made to a panel judge under this Ordinance.

(3) The Secretary for Security may from time to time revise the whole or any part of the code of practice, in a manner consistent with his power to issue the code under this section, and, unless the context otherwise requires, any reference to the code of practice, whether in this Ordinance or otherwise, is to be construed as a reference to the code as so revised.

(4) Any officer of a department shall, in performing any function under or for the purposes of any provision of this Ordinance, ~~have regard to~~ **comply with** the provisions of the code of practice.

(5) A failure on the part of any person to comply with any provision of the code of practice –

(a) is for all purposes not of itself to be regarded as a failure to comply with any provision of this Ordinance; and

(b) without prejudice to paragraph (a), does not affect the validity of any prescribed authorization or device retrieval warrant.

PART 6 MISCELLANEOUS

60. Prescribed authorizations and device retrieval warrants not affected by minor defects

(1) A prescribed authorization or device retrieval warrant is not affected by any minor defect in it.

(2) Without ~~prejudice to limiting~~ the generality of subsection (1), any information (including any protected product) obtained pursuant to a prescribed authorization is not by reason only of any minor defect in the prescribed authorization to be rendered

inadmissible in evidence in any proceedings before any court.

(3) For the purposes of this section, any reference to minor defect, in relation to a prescribed authorization or device retrieval warrant, includes any defect or irregularity, other than a substantial defect or irregularity, in or in connection with –

- (a) the issue, or the purported issue, of that prescribed authorization or device retrieval warrant or of a document purporting to be that prescribed authorization or device retrieval warrant; or
- (b) the execution, or the purported execution, of that prescribed authorization or device retrieval warrant or of a document purporting to be that prescribed authorization or device retrieval warrant.

61. Immunity

(1) Subject to subsection (2), a person shall not incur any civil or criminal liability by reason only of –

- (a) any conduct carried out pursuant to a prescribed authorization or device retrieval warrant (including any conduct incidental to such conduct);
- (b) his performance or purported performance in good faith of any function under this Ordinance; or
- (c) his compliance with a requirement made or purportedly made under this Ordinance.

(2) Nothing in subsection (1) affects any liability that is or may be incurred by any person by reason only of –

- (a) any entry onto any premises without permission; or
- (b) any interference with any property without permission.

62. Regulation

The Chief Executive in Council may, subject to the approval of the Legislative Council, make regulations for –

- (a) the better carrying out of the purposes of this Ordinance; and
- (b) without limiting the generality of paragraph (a), prescribing any matter which this Ordinance provides is, or may be, prescribed by regulation made under this section.

63. Amendment of Schedules

The Chief Executive in Council may, ~~by notice published in the Gazette,~~ subject to the approval of the Legislative Council, amend Schedules 1, 2, 3 and 4 by notice published in the Gazette.

64. Repeal and consequential amendments

(1) The Interception of Communications Ordinance (Cap. 532) is repealed.

(2) The enactments specified in Schedule 5 are amended as set out in that Schedule.

65. Transitional arrangements

(1) Where any materials have been obtained by or on behalf of any department by carrying out any telecommunications interception pursuant to an order issued or renewed before the commencement of this Ordinance under the provision then in force as section 33 of the Telecommunications Ordinance (Cap. 106), sections 56 ~~applies~~ and 58 ~~apply~~, with necessary modifications, to the materials, to the extent that they are any of the contents of the communication intercepted or a copy of such contents, ~~and to the relevant matters~~ as if –

(a) the order were a prescribed authorization issued or renewed under this Ordinance, and accordingly –

(i) the materials were, for the purposes of sections 56 ~~and 58~~ ~~respectively~~, protected product and telecommunications interception product; and

(ii) the application for the issue or renewal of the order were an application for the issue or renewal of a prescribed authorization under this Ordinance; and

(b) the purpose sought to be furthered by carrying out the operation required to be carried out under the order were the relevant purpose of the order.

(2) Subsection (1) is in addition to and not in derogation of section 23 of the Interpretation and General Clauses Ordinance (Cap. 1).

(3) In this section –

“copy” (文本), in relation to any contents of a communication referred to in subsection (1), means any of the following (whether or not in documentary form) –

(a) any copy, extract or summary of such contents ~~which identifies itself as such copy, extract or summary of such contents~~;

(b) any record referring to the telecommunications interception referred to in subsection (1) which is a record of the identity of any person who is the sender or intended recipient of the communication.;

~~“relevant matters” (有關事宜) –~~

~~(a) in relation to section 58(2), means any particulars as to the telecommunications interception referred to in subsection (1); and~~

~~(b) in relation to section 58(3), means any evidence or question which tends to suggest any of the following matters –~~

~~(i) that an application has been made for the issue or renewal of the order referred to in subsection (1);~~

~~(ii) that the order has been issued or renewed;~~

~~(iii) that any requirement has been imposed on any person to provide assistance for the execution of the order;~~
~~(iv) that any information has been obtained pursuant to the order.~~

66. Expiry

This Ordinance shall expire 2 years from the date that this Ordinance takes effect unless renewed by a resolution passed by the Legislative Council.

SCHEDULE 1 [ss. 2 & 63] DEPARTMENTS

PART 1

DEPARTMENTS SPECIFIED FOR INTERCEPTION, ETC.

1. Customs and Excise Department
2. Hong Kong Police Force
3. Independent Commission Against Corruption

PART 2

DEPARTMENTS SPECIFIED FOR COVERT SURVEILLANCE, ETC.

1. Customs and Excise Department
2. Hong Kong Police Force
3. Immigration Department
4. Independent Commission Against Corruption

SCHEDULE 2 [ss. 2, 6, 51 & 63] PROCEDURES OF, AND OTHER MATTERS RELATING TO, ~~PANEL~~ JUDGES

1. Provisions for consideration of applications by ~~panel judge~~ judges of the Court of First Instance and judges of the District Court

~~(1) A panel judge shall consider any application made to him under this Ordinance in private.~~

~~(2) Without prejudice to subsection (1), the~~ Any application made to a panel judge of the Court of First Instance or a judge of the District Court under this Ordinance may, where the ~~panel judge of the Court of First Instance or the judge of the District Court~~ so directs, be considered at any place other than within outside the court precincts at any place other than the premises of a department.

~~(3) The panel judge of the Court of First Instance or the judge of the District~~

Court may consider the application with or without a hearing as he considers appropriate.-

~~(3) Without prejudice to Division 5 of Part 3 of this Ordinance, nothing in this section prevents consideration of the application by the panel judge on the basis of written submissions made to him.~~

(4) Any hearing conducted by the ~~panel~~ judge of the Court of First Instance or by the judge of the District Court to consider the application is to be held in private.

2. Further powers of ~~panel~~ judges of the Court of First Instance and judges of the District Court

For the purpose of performing any of his functions under this Ordinance, a ~~panel~~ judges of the Court of First Instance and judges of the District Court may administer oaths and take affidavits.

3. Provisions for documents and records compiled by or made available to ~~panel~~ judge judges of the Court of First Instance or judges of the District Court

(1) A ~~panel judge~~ judge of the Court of First Instance or a judge of the District Court shall cause all documents and records compiled by, or made available to, him for any purpose related to the performance of any of his functions under this Ordinance to be kept in a packet sealed by his order, as soon as they are no longer immediately required for the purpose of performing any of his functions under this Ordinance.

(2) Notwithstanding subsection (1), a judge of the Court of First Instance or a judge of the District Court ~~panel judge~~ to whom any documents or records are made available in the circumstances described in that subsection shall –

(a) cause a copy of each of the documents or records so made available to him to be certified by affixing his seal to it and signing on it; and

(b) cause the copy so certified to be made available to the department concerned.

(3) Where any documents or records are kept in a packet under subsection (1) –

(a) the packet is to be kept in a secure place specified by a judge of the Court of First Instance or a judge of the District Court ~~panel judge~~;

(b) the packet may not be opened, and the documents or records may not be removed from the packet, except pursuant to an order of a panel judge made for the purpose of performing any of his functions under this Ordinance (including those performed at the request of the Commissioner under section 51(1A)); and

(c) the packet, and the documents or records, may not be destroyed except pursuant to an order of a judge of the Court of First Instance or a judge of the District Court ~~panel judge~~.

(4) Where any packet is opened pursuant to any order of a judge of the Court of First Instance or a judge of the District Court ~~panel judge~~ referred to in subsection (3)(b) –

(a) if any documents or records have been removed from the packet, the judge of

~~the Court of First Instance or the judge of the District Court panel judge~~ shall cause the documents or records to be returned to be kept in the packet, as soon as they are no longer immediately required for the purpose of performing any of his functions under this Ordinance; and

(b) the ~~judge of the Court of First Instance or the judge of the District Court= panel judge~~ shall cause the packet to be sealed by his order, as soon as access to the documents or records kept in it is no longer immediately required for the purpose of performing any of his functions under this Ordinance, and the provisions of subsection (3) apply, with necessary modifications, to the packet so sealed as they apply to the packet referred to in subsection (1).

(5) Nothing in this section prevents any of the documents and records referred to in subsection (1), or any copies of such documents and records, to be made available to the department concerned, whether for the purposes of any relevant written determination provision or ~~otherwise~~ pursuant to an order of a judge of the Court of First Instance or a judge of the District Court=panel judge.

(6) In this section, “relevant written determination provision” (有關書面決定條文) means section 9(3), 12(3), 24(5) (whether with or without reference to section 28 of this Ordinance), 27(5) or 33(3) of this Ordinance.

4. Panel judge to act judicially but not regarded as court

~~In performing any of his functions under this Ordinance, a panel judge shall act judicially and have the same powers, protection and immunities as a judge of the Court of First Instance has in relation to proceedings in that Court, although he is for all purposes not regarded as a court or a member of a court.~~

SCHEDULE 3 [ss. 8, 11, 14, 17, 20 & 63] REQUIREMENTS FOR AFFIDAVIT OR STATEMENT FOR APPLICATION FOR ISSUE OR RENEWAL OF PRESCRIBED AUTHORIZATION FOR INTERCEPTION OR COVERT SURVEILLANCE

PART 1 APPLICATION FOR ISSUE OF ~~JUDICIAL JUDGE’S~~ COURT OF FIRST INSTANCE AUTHORIZATION FOR INTERCEPTION

An affidavit supporting an application for the issue of a ~~judicial judge’s~~ Court of First Instance authorization for interception is to –

- (a) state which of the purposes specified in section 3(1)(a)(i) and (ii) of this Ordinance is sought to be furthered by carrying out the interception;
- (b) set out –

- (i) the form of the interception and the information sought to be obtained by carrying out the interception;
- (ii) if known, the identity of any person who is to be the subject of the interception;
- (iii) if known, particulars of the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying any communication that is to be intercepted;
- (iv) the proposed duration of the interception;
- (v) ~~the nature of, and an assessment of the immediacy and gravity of~~ the following information –
 - (A) where the purpose sought to be furthered by carrying out the interception is that specified in section 3(1)(a)(i) of this Ordinance, the nature of, and an assessment of the immediacy and gravity of, the particular serious crime to be prevented or detected; or
 - (B) where the purpose sought to be furthered by carrying out the interception is that specified in section 3(1)(a)(ii) of this Ordinance, the nature of, and an assessment of the immediacy and gravity of, the particular threat to public security, and an assessment of the impact, both direct and indirect, of the threat on the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong;
- (vi) the benefits likely to be obtained by carrying out the interception;
- (vii) an assessment of the impact (if any) of the interception on any person other than that referred to in subparagraph (ii);
- (viii) the likelihood that any information which may be subject to legal professional privilege, or may be journalistic material, will be obtained by carrying out the interception; ~~and~~
- (ix) the reason why the purpose sought to be furthered by carrying out the interception cannot reasonably be furthered by other less intrusive means; and
- (x) if known, whether, during the preceding 2 years, there has been any application for the issue or renewal of a prescribed authorization in which –
 - (A) any person set out in the affidavit under subparagraph (ii) has also been identified as the subject of the interception or covert surveillance concerned; or
 - (B) where the particulars of any telecommunications service have been set out in the affidavit under subparagraph (iii), the interception of any communication to or from that telecommunications service has also been sought, and if so, particulars of such application; and
- (c) identify by name, ~~and~~ rank and post the applicant and any officer of the department concerned approving the making of the application.

PART 2
APPLICATION FOR ISSUE OF ~~JUDICIAL JUDGE'S~~ COURT OF FIRST

INSTANCE
AUTHORIZATION FOR TYPE 1 SURVEILLANCE

An affidavit supporting an application for the issue of a ~~judicial judge's~~ Court of First Instance authorization for Type 1 surveillance is to –

- (a) state which of the purposes specified in section 3(1)(a)(i) and (ii) of this Ordinance is sought to be furthered by carrying out the Type 1 surveillance;
- (b) set out –
 - (i) the form of the Type 1 surveillance (including the kind or kinds of any devices to be used) and the information sought to be obtained by carrying out the Type 1 surveillance;
 - (ii) if known, the identity of any person who is to be the subject of the Type 1 surveillance;
 - (iii) the identity of any person, other than that referred to in subparagraph (ii), who may be affected by the Type 1 surveillance or, if the identity of such person is not known, the description of any such person or class of such persons who may be affected by the Type 1 surveillance;
 - (iv) if known, particulars of any premises or any object or class of objects in or on which the Type 1 surveillance is to be carried out;
 - (v) the proposed duration of the Type 1 surveillance;
 - (vi) ~~the nature of, and an assessment of the immediacy and gravity of the~~ following information –
 - (A) where the purpose sought to be furthered by carrying out the Type 1 surveillance is that specified in section 3(1)(a)(i) of this Ordinance, the nature of, and an assessment of the immediacy and gravity of, the particular serious crime to be prevented or detected; or
 - (B) where the purpose sought to be furthered by carrying out the Type 1 surveillance is that specified in section 3(1)(a)(ii) of this Ordinance, the nature of, and an assessment of the immediacy and gravity of, the particular threat to public security, and an assessment of the impact, both direct and indirect, of the threat on the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong;
 - (vii) the benefits likely to be obtained by carrying out the Type 1 surveillance;
 - (viii) an assessment of the impact (if any) of the Type 1 surveillance on any person referred to in subparagraph (iii);
 - (ix) the likelihood that any information which may be subject to legal professional privilege, or may be journalistic material, will be obtained by carrying out the Type 1 surveillance; ~~and~~
 - (x) the reason why the purpose sought to be furthered by carrying out the Type 1 surveillance cannot reasonably be furthered by other less intrusive means; and
 - (xi) if known, whether, during the preceding 2 years, there has been any application for the issue or renewal of a prescribed authorization in which any person set

- out in the affidavit under subparagraph (ii) has also been identified as the subject of the interception or covert surveillance concerned, and if so, particulars of such application; and
- (c) identify by name, ~~and~~ rank and post the applicant and any officer of the department concerned approving the making of the application.

PART 3
APPLICATION FOR ISSUE OF ~~EXECUTIVE~~ DISTRICT
COURT AUTHORIZATION
FOR TYPE 2 SURVEILLANCE

~~A statement~~ An affidavit supporting an application for the issue of a District Court ~~an executive~~ authorization for Type 2 surveillance is to –

- (a) state which of the purposes specified in section 3(1)(a)(i) and (ii) of this Ordinance is sought to be furthered by carrying out the Type 2 surveillance;
- (b) set out –
- (i) the form of the Type 2 surveillance (including the kind or kinds of any devices to be used) and the information sought to be obtained by carrying out the Type 2 surveillance;
 - (ii) if known, the identity of any person who is to be the subject of the Type 2 surveillance;
 - (iii) the identity of any person, other than that referred to in subparagraph (ii), who may be affected by the Type 2 surveillance or, if the identity of such person is not known, the description of any such person or class of such persons who may be affected by the Type 2 surveillance;
 - (iv) if known, particulars of any premises or any object or class of objects in or on which the Type 2 surveillance is to be carried out;
 - (v) the proposed duration of the Type 2 surveillance;
 - (vi) ~~the nature of, and an assessment of the immediacy and gravity of – the~~ following information –
 - (A) where the purpose sought to be furthered by carrying out the Type 2 surveillance is that specified in section 3(1)(a)(i) of this Ordinance, the nature of, and an assessment of the immediacy and gravity of, the particular serious crime to be prevented or detected; or
 - (B) where the purpose sought to be furthered by carrying out the Type 2 surveillance is that specified in section 3(1)(a)(ii) of this Ordinance, the nature of, and an assessment of the immediacy and gravity of, the particular threat to public security, and an assessment of the impact, both direct and indirect, of the threat on the security of Hong Kong, the residents of Hong Kong, or other persons in Hong Kong;
 - (vii) the benefits likely to be obtained by carrying out the Type 2 surveillance;
 - (viii) an assessment of the impact (if any) of the Type 2 surveillance on any person referred to in subparagraph (iii);

- (ix) the likelihood that any information which may be subject to legal professional privilege, or may be journalistic material, will be obtained by carrying out the Type 2 surveillance; ~~and~~
 - (x) the reason why the purpose sought to be furthered by carrying out the Type 2 surveillance cannot reasonably be furthered by other less intrusive means; and
 - (xi) if known, whether, during the preceding 2 years, there has been any application for the issue or renewal of a prescribed authorization in which any person set out in the ~~statement~~ affidavit under subparagraph (ii) has also been identified as the subject of the interception or covert surveillance concerned, and if so, particulars of such application; and
- (c) identify by name, ~~and~~ rank and post the applicant.

PART 4
APPLICATION FOR RENEWAL OF ~~JUDICIAL JUDGE'S~~ COURT OF FIRST INSTANCE
AUTHORIZATION OR ~~EXECUTIVE~~ DISTRICT COURT AUTHORIZATION
FOR
INTERCEPTION OR COVERT SURVEILLANCE

An affidavit ~~or statement~~ supporting an application for the renewal of a ~~judicial judge's~~ Court of First Instance authorization for interception or Type 1 surveillance or a District Court ~~an executive~~ authorization for Type 2 surveillance is to –

- (a) set out –
 - (i) whether the renewal sought is the first renewal and, if not, each occasion on which the ~~judicial judge's~~ Court of First Instance authorization or a District Court ~~an executive~~ authorization has been renewed previously;
 - (ii) any significant change to any information previously provided in any affidavit ~~or statement~~ under this Ordinance for the purposes of any application for the issue or renewal of the ~~judicial judge's~~ Court of First Instance authorization or a District Court ~~an executive~~ authorization; ~~or for the purposes of any application made further to an oral application for confirmation of the judicial judge's authorization or executive authorization or its previous renewal;~~
 - (iii) an assessment of the value of the information so far obtained pursuant to the ~~judicial judge's~~ Court of First Instance authorization or a District Court ~~an executive~~ authorization;
 - (iv) the reason why it is necessary to apply for the renewal; and
 - (v) the proposed duration of the interception, Type 1 surveillance or Type 2 surveillance (as the case may be); and
- (b) identify by name, ~~and~~ rank and post the applicant and any officer of the department concerned approving the making of the application.

REQUIREMENTS FOR AFFIDAVIT FOR APPLICATION FOR ISSUE OF DEVICE RETRIEVAL WARRANT

An affidavit supporting an application for the issue of a device retrieval warrant for the retrieval of any of the devices authorized to be used under a prescribed authorization is to –

(a) set out –

- (i) the kind or kinds of the devices sought to be retrieved;
- (ii) particulars of the premises or object from which the devices are to be retrieved, and the reason why the applicant considers that the devices are in or on such premises or object;
- (iii) the estimated time required to complete the retrieval;
- (iv) an assessment of the impact (if any) of the retrieval on any person;
- (v) an assessment of the risk and damage arising from the retrieval of the devices before the termination of the authorization; and

(~~v~~vi) the need for the retrieval; and

(b) identify by name, ~~and~~ rank and post the applicant.

SCHEDULE 5 [s. 64] CONSEQUENTIAL AMENDMENTS

Post Office Ordinance

1. Warrant of Chief Secretary for Administration 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, 12 or 13

(1) Section 14 is amended, in the heading, by repealing “, 12 or 13” and substituting “or 12”.

(2) Section 14 is amended by repealing “, 12 or 13” and substituting “or 12”.

3. Extension of sections 12, 13 and 14 to articles not transmissible by post

(1) Section 15 is amended, in the heading, by repealing “, 13”.

(2) Section 15 is amended by repealing “, 13”.

Post Office Regulations

4. Regulation amended

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

Telecommunications Ordinance

5. Section substituted

Section 33 of the Telecommunications Ordinance (Cap. 106) is repealed and the following substituted –

“33. Orders for interception of messages for provision of facilities

(1) For the purpose of providing or making available facilities reasonably required for –

(a) the detection or discovery of any telecommunications service provided in contravention of any provision of this Ordinance or any regulation made under this Ordinance or any of the terms or conditions of a licence granted under this Ordinance; or

~~(b) the execution of prescribed authorizations for telecommunications interception that may from time to time be issued or renewed under the Interception of Communications and Surveillance Ordinance (of 2006),~~ the Chief Executive may order that any class of messages shall be intercepted.

(2) An order under subsection (1) shall not of itself authorize the obtaining of the contents of any individual message.

(3) In this section –

“contents” (内容), in relation to any message, has the meaning assigned to it in section 2(5) of the Interception of Communications and Surveillance Ordinance (of 2006) in relation to a communication referred to in that section;

“prescribed authorization” (訂明授權) has the meaning assigned to it in section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

“telecommunications interception” (電訊截取) has the meaning assigned to it in section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006).”.

Prevention of Bribery Ordinance

6. Public bodies

Schedule 1 to the Prevention of Bribery Ordinance (Cap. 201) is amended by adding –
“107. Commissioner on Interception of Communications and Surveillance.”.

Personal Data (Privacy) Ordinance

7. Section added

The Personal Data (Privacy) Ordinance (Cap. 486) is amended by adding –

“58A. Protected product and relevant records under Interception of Communications and Surveillance Ordinance

(1) A personal data system is exempt from the provisions of this Ordinance to the extent that it is used by a data user for the collection, holding, processing or use of personal data which are, or are contained in, protected product or relevant records.

(2) Personal data which are, or are contained in, protected product or relevant records are exempt from the provisions of this Ordinance.

(3) In this section –

“device retrieval warrant” (器材取出手令) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

“prescribed authorization” (訂明授權) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

“protected product” (受保護成果) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (of 2006);

“relevant records” (有關紀錄) means documents and records relating to –

(a) any application for the issue or renewal of any prescribed authorization or device retrieval warrant under the Interception of Communications and Surveillance Ordinance (of 2006); or

(b) any prescribed authorization or device retrieval warrant issued or renewed under that Ordinance (including anything done pursuant to or in relation to such prescribed authorization or device retrieval warrant).”.

Official Secrets Ordinance

8. Information related to commission of offences and criminal investigations

Section 17(2)(c), (d) and (e) of the Official Secrets Ordinance (Cap. 521) is repealed and the following substituted –

“(c) any information, document or article which is interception product within the meaning of the Interception of Communications and Surveillance Ordinance (of 2006); or

(d) any information relating to the obtaining of any interception product described in paragraph (c).”.