立法會
Legislative Council

LC Paper No. CB(2)2837/05-06

Ref : CB2/BC/2/05

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 –

	Subject	Paragraphs
(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 an 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.

<u>Surveillance device</u>

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 the following –

(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 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 cause to be 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 cause to be 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.

<u>Regular review</u>

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) covers 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.

<u>Non-compliance with the provisions in the Bill or the code of practice</u>

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.

<u>Notification of targets of interception of communications or surveillance</u>

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 increasing 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 knowing 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.

248. Apart from the CSAs discussed in the above paragraphs, Hon Margaret NG has proposed other amendments to the Bill.

249. Apart from the CSAs discussed in the above paragraphs, Hon James TO has proposed other amendments to the Bill.

Follow-up actions by the Administration

250. 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

251. 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).

Consultation with the House Committee

252. The Bill Committee consulted the House Committee on 21 July 2006 and sought the latter's agreement that the Second Reading debate on the Bill be resumed at the Council meeting on 2 August 2006.

Council Business Division 2
Legislative Council Secretariat
28 July 2006

Appendix I

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

Appendix II

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